Kevin Daimi
Ioanna Dionysiou
Nour El Madhoun *Editors*

Principles and Practice of Blockchains

Springer

Principles and Practice of Blockchains

Kevin Daimi • Ioanna Dionysiou •
Nour El Madhoun
Editors

Principles and Practice of Blockchains

Springer

Editors

Kevin Daimi
University of Detroit Mercy
Detroit, MI, USA

Ioanna Dionysiou
Department of Computer Science
University of Nicosia
Nicosia, Cyprus

Nour El Madhoun
EPITA Engineering School
Le Kremlin-Bicêtre, France

ISBN 978-3-031-10506-7 ISBN 978-3-031-10507-4 (eBook)
https://doi.org/10.1007/978-3-031-10507-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Blockchain is considered as distributed records or lists assigned to network nodes. They store information in blocks where each block is linked to the previous one. These blocks establish a chain (blockchain). Initially, blockchains were created for cryptocurrency systems to sustain a secure and decentralized collection of transactions. Soon after, many different applications of blockchains emerged.

Financial systems depend on key agencies and trustworthy intermediaries to smoothen the progress of business transactions. Blockchain as a technology minimizes the need for such authorities. Blockchain assists in the authentication and trackability of various transactions that need verification and traceability. It can ensure secure transactions, minimize compliance costs, and accelerate data transfer handling. The technology can assist in managing contracts and the auditing of the source of an artifact.

Principles and Practice of Blockchains provides an essential compilation of relevant and cutting-edge academic and industry work on key blockchain topics. Further, it introduces blockchains to the public at large to develop their blockchain knowledge and awareness. The book can be a valuable resource to blockchain experts towards their professional development efforts and to students as a supplement to their cybersecurity courses. It provides a glimpse of future directions where blockchains are heading. The book is a rich collection of carefully selected and reviewed manuscripts written by diverse blockchain experts in the listed fields and edited by prominent blockchain researchers and specialists.

The first part of the book covers blockchain fundamentals. It starts by explaning consensus protocols, smart contracts, and decentralized applications. It then introduces a quantitative description of several experiments conducted with the goal of investigating the elliptic dataset, and multidimensional blockchain and its peculiarities including inner search and verification protocol for blocks and transactions. The part concludes with an illustration of information workflow mechanism for inter-organizational collaboration enforced via smart contract and deployed on the blockchain network.

Part II concentrates on Internet of Things (IoT) and mobile phones. The location privacy preservation problem in the context of both permissionless and permissioned blockchain-based IoT systems is studied and quantified by considering the scope of key distribution tasks, spatiotemporal correlation among location-based transactions, and communication medium among the IoT devices. A blockchain-based machine learning intrusion detection system for Internet of Things is later introduced. This is then followed by a proof-of-concept prototype that is implemented and evaluated on a physical network that uses Raspberry Pis to simulate IoT devices. The last chapter in this part examines the relevancy of value dimensions and the trustworthiness of blockchain-based mobile phone applications (BMPAs). Using the dimension of customer value and customer behavior, the chapter recommends a customer outcome framework for businesses that adopt the BMPAs.

Healthcare is a growing area for blockchains. Part III examines a blockchain structure to develop a decentralized and secured healthcare system. The system ensures that patients personalize and govern their healthcare data while others are considered client with assigned liberty. Furthermore, a review on existing initiatives, frameworks, theoretical research, and practical implementations of the blockchain and smart contracts technologies in the healthcare industry's facilities and activities as well as a critical assessment of the security aspects of the various solutions related to smart medicine of blockchain-based solutions are presented.

Part IV concentrates on the traditional use of blockchain. The first chapter in this part presents a study of the main challenges associated with the design of a quantum-resistant version of bitcoin that is based on any of the post-quantum digital signatures selected as finalists and alternates of NIST third-round post-quantum cryptography standardization process. The second chapter depicts an overview and comparison of traditional and cyber money laundering methods and operationally compares traditional and cyber money laundering. It also covers existing legal and regulatory frameworks, identifies areas of necessary improvement, and proposes potential technical and non-technical anti-cyber laundering remedies.

The last part of this book deals with blockchains in education, governance, supply chain, and security. Education is covered via a blockchain-based homework grading system to establish a transparent and fair platform for teacher-student interactions. The goal is to ensure the fairness and transparency of the mutual interaction between students and teachers to guarantee that all students are being treated equally in grading. The next chapter focuses on the application of blockchain technology in a supply chain to improve business performance and discusses the benefits and challenges of blockchain technology in supply chain management. The corporate governance chapter proposes a reflection on the relationship between blockchain technology and corporate governance based on a review of the literature and presents a review of the theoretical and empirical evidence of this relationship. The book is concluded by the chapter on sociotechnical security of blockchain technology that introduces the notion of "people security" to argue that blockchains hold inherent limitations in offering accurate security guarantees to people as participants in blockchain-based infrastructure due to the differing nature of the threats to participants reliant on blockchain as secure digital infrastructure, as well as the technical limitations between different types of blockchain architecture.

The editors of *Principles and Practice of Blockchains* are humbled to provide a book that covers the state, principles, practice, methods, algorithms, techniques, and applications of blockchains to furnish an excellent professional development resource for educators and practitioners on the state-of-the-art blockchain materials and contribute towards the enhancement of the community outreach and engagement component of blockchains.

Acknowledgments

This book could not have emerged without the collaboration of many individuals. It gives us great pleasure to thank the authors of the chapters who spent enormous time working on producing their chapters and improving them based on the reviewers and editors' comments. We are indebted to our reviewers who invested their time, knowledge, and expertise in reviewing the book chapters. We are grateful to Mary James, Zoe Kennedy, and Brian Halm at Springer for their kind help and support.

Aida Kammoun Abdelmoula, University of Sfax, Tunisia
Mohammed Akour, Yarmouk Universitym Jordan
Rachid Boudour, Badji Mokhtar-Annaba University, Algeria
Yu Chen, Binghamton University, USA
Kevin Daimi, University of Detroit Mercy, USA
George Dimitoglou, Hood College, USA
Ioanna Dionysiou, University of Nicosia, Cyprus
Yeap Peik Foong, University of Newcastle, Australia
Harald Gjermundrod, University of Nicosia, Cyprus
Line Guffond Le Goanvic, 360 V&P, France
Badis Hammi, EPITA, France
Elias Iosif, Institute for the Future, University of Nicosia, Cyprus
Jaspreet Kaur, Indian Institute of Technology Jodhpur, India
Rida Khatoun, Telecom-ParisTech, France
Nour El Madhoun, EPITA Engineering School, France
Kelsie Nabben, RMIT University, Australia
Saurav Negi, Modern College of Business and Science, Oman
Jenny Torres, Escuela Politécnica Nacional (EPN), Ecuador
Patrice Van De Velde, Unblocked, France
Ja Ling Wu, National Taiwan University, Taiwan

Contents

Part I Blockchain Fundamentals

Part II Blockchains in Internet of Things and Mobile Phones

Part III Blockchains and Healthcare

Part IV Blockchains and Currency

Part V Blockchains in Education, Governance, Supply Chain, and Security

About the Editors

Kevin Daimi received his PhD from the University of Cranfield, England. He has a long academic and industry experience. His research interests include computer and network security with emphasis on vehicle network security, software engineering, data science, and computer science and software engineering education. He has published a number of papers on vehicle security. He is the editor of three books in cybersecurity: *Computer and Network Security Essentials*, *Innovation in Cybersecurity Education*, and *Advances in Cybersecurity Management* which were published by Springer. He has been chairing the annual International Conference on Security and Management (SAM) since 2012. He is also program chair of the 2022 International Conference on Innovations in Computing Research (ICR'22), Athens, Greece. Kevin is a senior member of the Association for Computing Machinery (ACM), a senior member of the Institute of Electrical and Electronic Engineers (IEEE), and a fellow of the British Computer Society (BCS). He is the recipient of the Outstanding Achievement Award from the 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP'10) in Recognition and Appreciation of his Leadership, Service and Research Contributions to the Field of Network Security. He is currently Professor Emeritus of Computer Science and Software Engineering at the University of Detroit Mercy.

Ioanna Dionysiou is Professor of Computer Science at the University of Nicosia. She is currently the associate head of the Department of Computer Science. Dionysiou received her PhD from Washington State University (2006), and during her graduate studies, she held teaching and research assistant appointments. Her PhD dissertation work investigated trust requirements and challenges for large-scale infrastructures, with an exemplary infrastructure being the US Electric Power Grid. Dionysiou's research focuses on active defenses, privacy, applied security standards, multidisciplinary security practices, and cybercrime. She is the co-director of the Informatics Security Laboratory (ISL) at the University of Nicosia, which aims on devising new techniques to detect cyberattacks by analyzing attack patterns and visualizing attack attempts in an intuitive manner. She is member of various boards, including the Cyprus ECSC (European Cyber Security Challenge) Advisory Board. She has participated in locally funded and European-funded research projects.

Nour El Madhoun received her master's degree in networks/computer science from Sorbonne Université/Télécom ParisTech in 2014, and her PhD degree in cybersecurity/computer science from Sorbonne Université in 2018. In 2019, she joined ISEP – School of Digital Engineers, Paris, as Associate Professor of Cybersecurity in addition to overseeing the engineering cycle – Digital Security and Networks. In 2018, Nour gained industry experience by working as a postdoctoral researcher at Orange Labs. At Sorbonne Université, she became an ATER in 2017. From 2020 to 2022, Nour joined EPITA engineering school in Paris as Associate Professor of Cybersecurity and Blockchain. Her current research focuses on network security, cryptographic protocols, EMV payment, NFC technology, and blockchain and smart-contracts technologies. Nour is currently Associate Professor of Computer Science, Cybersecurity, and Blockchain at ISEP – School of Digital Engineers, Paris. She is also an associate researcher at Sorbonne Université (LIP6-PHARE Team).

Part I
Blockchain Fundamentals

Fundamentals of Blockchain Technology

Daniel Maldonado-Ruiz, Jenny Torres, and Nour El Madhoun

1 Introduction

When the Bitcoin white paper was published, the novel cryptocurrency offered not only a transparent handling of transactions made with the new cryptocurrency but also to solve the problem of double spending: the use or the spend of the same digital asset by two different and independent transactions (the digital version of money forgery). In order to do this, Bitcoin made use of the development of a ledger that could store all transactions via peer-to-peer methods, making them public and transparent to every user on the network. This was the best way to avoid having a trusted third party (TTP) to review and validate transactions. In fact, this was the first implementation of a fully functional blockchain as we understand it today. Even though blockchain was not a new technology per se, it made blockchain a trend in decentralisation and a tipping point for understanding modern peer-to-peer interactions [1, 2].

Since then, there were two branches of blockchain developments: the first is based on transactions represented by Bitcoin and other cryptocurrencies and is known as Blockchain 1.0. The second is based on storing of multiple types of information and programmable features, also known as the smart contract paradigm or Blockchain 2.0, where Ethereum is the main representative blockchain

D. Maldonado-Ruiz (✉) · J. Torres
Departamento de Informática y Ciencias de la Computación, Facultad de Ingeniería en Sistemas, Informáticos y Computación, Escuela Politécnica Nacional, Ecuador, Quito, Ecuador
e-mail: daniel.maldonado02@epn.edu.ec; jenny.torres@epn.edu.ec

N. E. Madhoun
EPITA Engineering School, Le Kremlin-Bicêtre, France
e-mail: nour.el-madhoun@lip6.fr; nour.el-madhoun@epita.fr

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_1

distribution. Both developments are applications of the same principle: an interconnected succession of information-storing blocks related to the previous one by cryptographic tools that make the chain an immutable ledger [3, 4].

In the last few years, blockchain technology has received an increasing attention in several areas such as electronic voting, healthcare, insurance or data verification for several types of information technology (IT) applications (explained in Sect. 5) because of its features of tamper-resistant distributed storage system. With this attention, it comes a 'hype' where blockchain is made to appear as the solution to all the problems that may arise in the network. However, the use of blockchain technology to implement in an IT application requires the consideration of several conditions, the first of them is the capability of the network to decentralise their storage infrastructure and the information to be accessible for every interested user [5].

In centralised environments, the communication between users and the exchange of information need to be regulated by a TTP, acting like the handler of every communication and enabling the verification of every exchange. Instead, every distributed communication, specially blockchain, allows the exchange without the mandatory validation by the TTPs or any of the centralised security layers associated with them. With the same concepts of P2P interactions, blockchain handles the communication only between the other users but implements several security distributed layers to secure every communication, as well as smart contract technology that allows the automation of agreements between users [6–8].

Blockchain is based on the *'non-intervention of a central regulation entity in every interaction between user'* concept, which represents that each transaction is the responsibility, in creation and transmission, of each user, while validation and acceptance are supported by network algorithms. That is, much of the system's trust is based on the network itself, implicitly, rather than on any explicit authority. Not all the IT applications can be suitable to implement all the benefits of blockchain. In this chapter, we present all the concept features that allow blockchain to create decentralised, secure and transparent networks and in which application this technology is suitable to create a new paradigm of information [9].

2 Blockchain Features and Architecture

A blockchain is a set of linked blocks where the creation of a block requires data from the previous one, creating an immutable link between them. For that, blockchain needs a process to create and link new blocks to the ledger safely. Figure 1 shows how a block is created. This process is analogue in all known blockchains, even when block types and capabilities of every block are different. When a user A needs to transact with another user B, the transaction is created (1) and then stored (2) in a temporary buffer with the other transactions from other users. These transactions are validated and turned into a block, with a variable number of transactions per block. The validation/block creation is accomplished by a third independent user known as a miner (3). The miner is a type of user (or

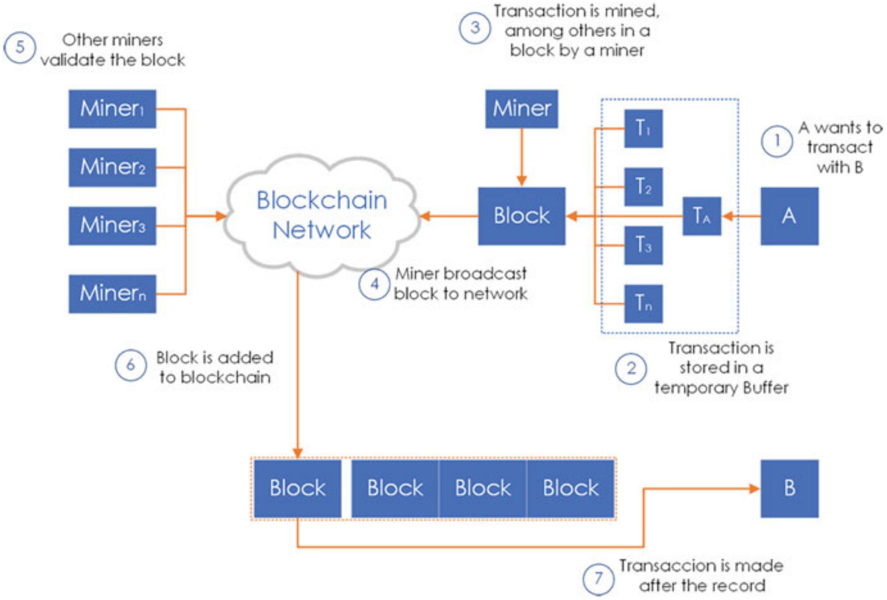

5 Other miners validate the block
3 Transaction is mined, among others in a block by a miner
Miner1
Miner2
Miner3
Minern
Blockchain Network
Miner
Block
T1
T2
TA
T3
Tn
A
1 A wants to transact with B
4 Miner broadcast block to network
6 Block is added to blockchain
2 Transaction is stored in a temporary Buffer
Block
Block
Block
Block
B
7 Transaccion is made after the record

Fig. 1 Blockchain block creation [10]

node) that inverts computational time to group several transactions together and turn them into a block. After the creation, the new block is broadcast on the network (4) and the other nodes in the network check the validity of this new block (5), and after validation, this new block will be added to the blockchain (6). From the new block, the user *B* can validate the transaction made by *A* and finally receive the currency [4, 10].

In order to study how a blockchain is implemented besides the basic theory shown in Figs. 1 and 2 shows the blockchain layer architecture, which explains how every blockchain operational function is grouped and classified, layer by layer. This layer division is important to understand how 'physical' structures, like Merkle trees or hash functions (Layer 1), build the system that will be broadcast by the network layer (Layer 2) and trusted by the consensus layer (Layer 3). The definitions of Layers 1 and 2 are beyond the scope of this chapter, so the explanation of how blockchain works will start with Layer 3. One of the main features of blockchain is that it allows users to interact even if they do not trust each other (at the beginning or during the transaction). This means that when users transact with each other, the trust is based only on the network and the functions specified in the first three layers [10].

The network *internal trust* allows each user, also known as a node, to read, write, create, validate and interact with the network, without worrying about other users or transactions. This internal trust is achieved in blockchain using an algorithm that prevents malicious users/nodes from gaining access to the network and hijacking the

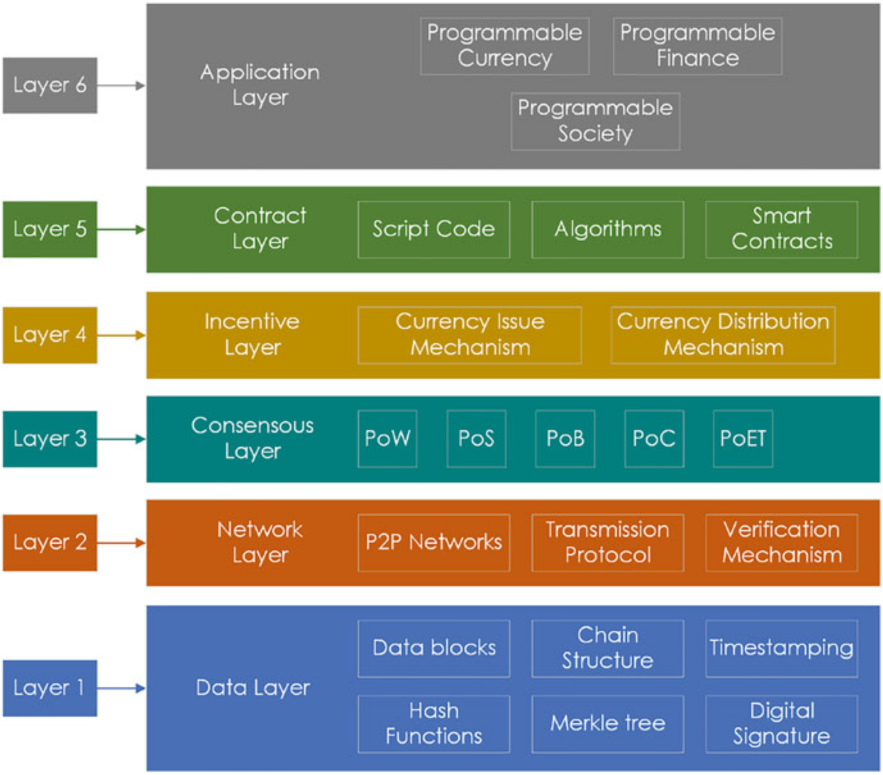


Fig. 2 Blockchain layer architecture [10]

internal trust. The process that makes the trust possible is based on the Byzantine General problem and is called *consensus*. The consensus algorithms allow users to create and validate new blocks with the confidence that all blocks are true by relying only on the internal processes of the network. In addition, consensus prevents the blockchain network from creating unwanted or fraudulent branches when adding new blocks, maintaining the blockchain as a unique decentralised structure [11].

There are several types of consensus algorithms, and the most common implementations are proof of work (PoW) and proof of stake (PoS):

2.1 Proof of Work (PoW)

It is the first and most extensive consensus algorithm used in the blockchain world. Deployed originally for Bitcoin, it is based on the work of untrustworthy nodes and public networks. PoW has the particularity of allowing only one 'winner' to involve in the generation process of the block. This means that, even when all the nodes in the network can create the correct block to be stored on the blockchain, only one block is considered valid. All other coincidences created by other nodes are discarded. When a new block is about to be created, several nodes (or groups of nodes) challenge the network to achieve the creation of the new block. This is illustrated in Fig. 1, where nodes use some of the transactions stored in the temporal data buffer and attempt to create a block using their computational power to guess a unique number called *nonce*, which is part of the header of every block. In this process, the nodes compete with each other to find the right nonce ahead of other ones. This nonce, hashed with all the block, makes the entire block complex enough to be equivalent to some predefined complexity threshold. The competition to find the right nonce, and therefore a valid block, is known as mining. The first node to achieve the mining 'wins' the creation of the block [1, 10, 12].

Several, if not all the miners in the network, can create the same block. All the miners must compete to store their block in the blockchain, as shown in Fig. 3a,

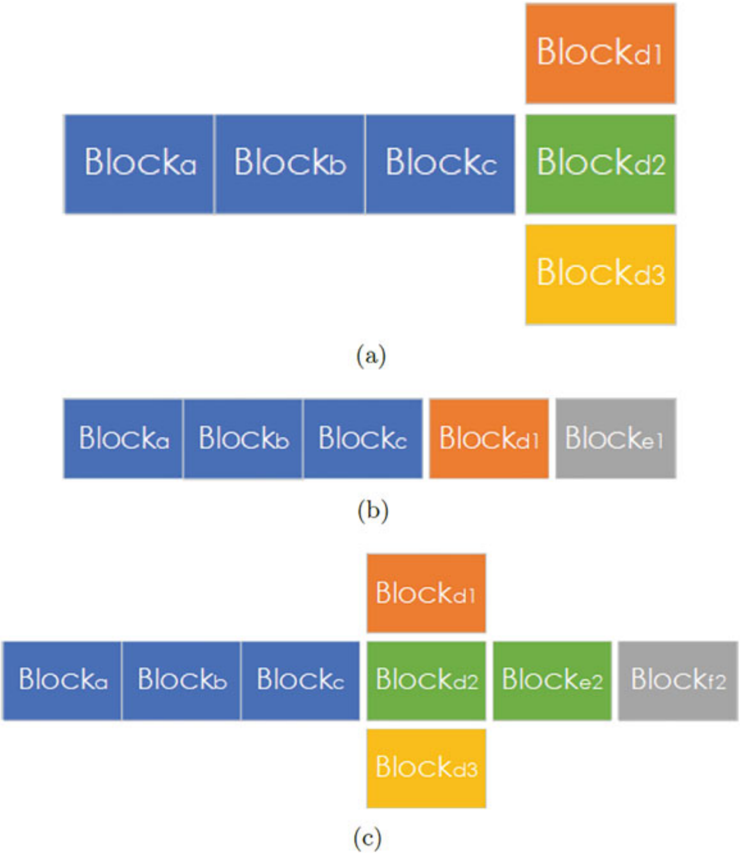


Fig. 3 Longest chain creation. (**a**) Blockchain mining blocks creation. (**b**) Creation of following blocks. (**c**) Consolidation of the Longest Chain

where different blocks (created by different miners) compete to be the block *d*. The miner attempting to create the next block (*e*) must perform two tasks before creating the new block: (a) create the next block following a specific branch, which means a block that follows the chain of some previous block chosen as a landmark and (b) check the network to see if the chosen branch selected by the miner is still part of the canonical network. For example, Fig. 3b illustrates how the miner assumes that *Block d1* (chosen as landmark) is the valid block in the blockchain and so the *Block e1* must be the next block to be created. But this node must be sure that the chain that it is creating is the valid chain for every node in the network. The problem is how the miner knows which chain is valid. PoW defines the chain validation by the 'longest chain' rule. Before creating a new block, miners must perform a double validation on the network to know which block is a part of the longest chain. Figure 3c shows how the longest chain consolidates. After the challenge, the nodes know which blocks are part of the longest chain. The 'winning' miners finally add the new blocks they created to the valid chain. With this method, the Bitcoin blockchain can avoid any central validation of miners and trust the network to remain valid on its own.

Because the trustworthiness of the entire network is based within the network and not in the nodes, every miner is considered as an anonymous party in the network. In other words, besides their addresses to receive the mining fees, the miners do not need to share any identification to engage in mining or in the validation of the new created blocks. Most public blockchains use this consensus protocol to maintain full decentralisation of the network and full anonymity in every transaction.

2.2 *Proof of Stake (PoS)*

It is currently implemented on Ethereum Casper and Ethereum 2.0 blockchains and is designed to avoid the anonymity issues of PoW. Moreover, PoW has several electricity consumption issues, which are solved with PoS to avoid the random competition of the nodes. PoS allows blocks to be created only by nodes that can be validated from the network. These nodes are called validators. Each validator creates its chance to produce the new block by determining (a) how many coins or tokens are in its wallet and (b) how many of those coins or tokens can be locked as a stake for the creation of the new block. This means that the biggest stake has the greatest chance of being the creator of the new block. As for the other validators that can create the same block (as happens on PoW), and instead of competing to be the longest chain, they combine their blocks as one and each creator receives a reward based on each stack made for the block. This way, the mining actions in the network are improved, as every effort has a reward and also avoids any unnecessary branches in the blockchain [10, 12, 13].

One of the main issues of PoS lies precisely in the principle of creating new blocks. A user with sufficient capacity to contribute tokens could effectively 'purchase' most of the chances for the creation of new blocks, which would defeat the decentralisation principle of blockchain in the creation of new blocks, and

Table 1 Comparison between PoW and PoS

	PoW	PoS
Security	It is needed the 51% of computational power to tamper the network	It is needed the 51% of the total stake to tamper the network
Decentralisation	Miners 'win' the creation chance by executing mathematical problems. Full decentralised system	The user with the more stake in the network can 'purchase' their chances to create a block
Energy consumption	High	Comparatively low
Participation costs	Every miner needs to invest in energy and computational equipment to create a block	Every validator needs to invest cryptocurrency to create a block

turning that user as the master of the network, which would defeat the principle of equality among the validators.

Both PoW and PoS are the main consensus protocols used in many mainstream implementations of blockchain because they are the fundamentals of Bitcoin and Ethereum (Ethereum 2.0 implements PoS widely to replace PoW in the new fork). Table 1 shows how these two protocols are related, focusing on the energy and security features, which are the most important consideration in a new implementation.

There are other consensus algorithms slightly based on the PoS concept and more scarcely implemented but are still part of the new research on blockchain and consensus and which are classified by the resource that is used to increase the probability of creating the block. The most important ones are:

2.3 *Proof of Burn (PoB)*

Instead of using a stake, validators on PoB 'burn' their cryptocurrency or tokens at an unreachable but public and verifiable address, also known as eater address, to have their chances to create the new block. Unlike PoS, the burned cryptocurrency is not returned to the validator even if it created the valid block. The fund address 'eats' every token stored, making it unreachable for its previous owner. Instead, it remains as a fund to create the trust needed to create more blocks. In a way, every validator must invest in the blockchain in order to show the commitment with the network and its growing [12, 14].

PoB was created to improve PoW, in order to avoid the limitations of acquisition of the processing power needed to create new blocks in traditional blockchain. Instead, the resource choses the cryptocurrency associated with the system that is used to ensure the possibility of creating new blocks. The acquisition of the aforementioned cryptocurrency is independent of the creation of the blocks. A user could use real money to acquire the amount of tokens needed to secure their place in the block creation. Every block creation is an investment performed by the validator.

However, PoB has several disadvantages over its utilisation. The first is financial, since like any investment, the validator may lose the tokens invested if he/she does not reach sufficient tokens to ensure the creation of new blocks. And also, a validator can 'purchase' their chance of creation every time, braking the decentralisation concept of the entire network.

The most important cryptocurrency scheme using PoB is SlimCoin, an open-source cryptocurrency that is currently in the development phase by its community. Besides PoB, SlimCoin uses PoW and PoS as consensus protocols, being the first cryptocurrency to use three native protocols in their block creation process[15].

2.4 *Proof of Capacity (PoC)*

It is also known as proof of space. Instead of using cryptocurrency to lock the block creation chance, PoC uses node's hard disc space or RAM-type memory (a computational space where the consensus files/processes can be stored) to generate their capacity and ability to create a block in a blockchain. When PoC is performed, a list of possible solutions of the mining process are stored into the computational space used to mining. The larger the computational space designed, the list of possible solutions is bigger, and therefore, the chances to have the correct solution of the mining process are larger [16, 17].

This list of possible solutions are nonces result of successive hashing processes of user-related data. According to [17], each nonce contains 8192 hashes, every one of them related to their adjacent (0–1, 2–3 and so on) into a tuple called 'scoop' (there are 8192 hashes and 4096 scoops). The mining process consists of calculating one of the scoops and with the scoop calculate what is called a 'deadline value'. A deadline is basically the amount of time (in seconds) between the creation of the last block and the new one. The process to calculate the deadline is repeated until it found the minimum deadline based on the nonces stored in the computational space. If, during the calculated period of time, no other miner creates a block in the blockchain, the miner wins the possibility and creates the new block.

This mining process has proven to be energy efficient compared to other mining processes, as well as running on any system that runs on physical computing space, including smartphones. Additionally, the computational space used to store the list of nonces is not permanently compromised, allowing the device's RAM or storage space to be reused without inconvenience. Nevertheless, PoC as being stored on hard discs or RAM slots, it is vulnerable to malware attacks or other attacks where the storage is compromised. Additionally, its implementation is not so easy as PoW or PoS, so not many developers have implemented this protocol. PoC is mostly implemented in SpaceMint, a Bitcoin-related cryptocurrency which bases all the implementation of their blockchain in PoC, establishing the condition to reward the miners to maintain the blockchain [18].

2.5 *Proof of Elapsed Time (PoET)*

Emulating a time-division multiplexing system, PoET is a theoretical consensus protocol proposed by Intel and developed over Hyperledger in 2016, which gives each node a randomly chosen time slot to create its block, while the other nodes are registered as waiting nodes (waiting for their turn in validating the new block). If the node spends the least amount of time when creating the block, it is considered the winner for being attached to the chain. This time slot is assigned randomly to a node, avoiding the competition between the nodes and obviously reducing the power consumption of the whole network. In fact, PoET must assure the true randomness of the time slots (not only the assignment of a slot in a way that the users can choose one suitable slot for the block creation) and that the user which creates the block effectively uses all the time assigned to it (called waiting time) to create the block [10, 19].

The only application known for PoET is Sawtooth, which currently is under development, and no other blockchain or cryptocurrency uses this PoW variation consensus protocol.

All current blockchains work with the first three layers as shown in Fig. 2 and implement, through miners or validators, several systems of rewards for the creation of blocks, paid in Bitcoins for the miners or in gas for the validators, in order to keep users incentivised in the maintenance and upkeep of the network. These processes are grouped in Layer 4. Each block created and consolidated generates a reward to encourage the creation of new blocks. The last two layers, the contract layer (Layer 5) and the application layer (Layer 6) shown in Fig. 2, are the creations of Ethereum blockchain and of its derivatives as well, where the chain evolves and allows generating a new type of blockchain, known as Blockchain 3.0, where not only information will tamper-proof but also the company involved in the blockchain and its records [1, 3, 4, 13].

Figure 4 shows the main structure of a blockchain block, where the header and the body are two different structures, not only in terms of size but also in terms of hash execution. The body of the block contains all the transactions that have been recorded and confirmed by the network. The number of transactions on the block is variable, and every transaction needs to be tracked individually inside the block, which makes it impossible to use a classical hash algorithm, such as SHA-256. Consequently, the transactions use Merkle Hash Trees. The header, on the other hand, always has the same size, containing the SHA-256 or similar hash of itself, the hash of the previous block header, the nonce used for PoW, a creation timestamp, and the final Merkle hash tree for the body. Every block in every blockchain, regardless of its development, contains the same structure. This provides an easy way to find information about transactions or smart contracts across all blockchains [12].

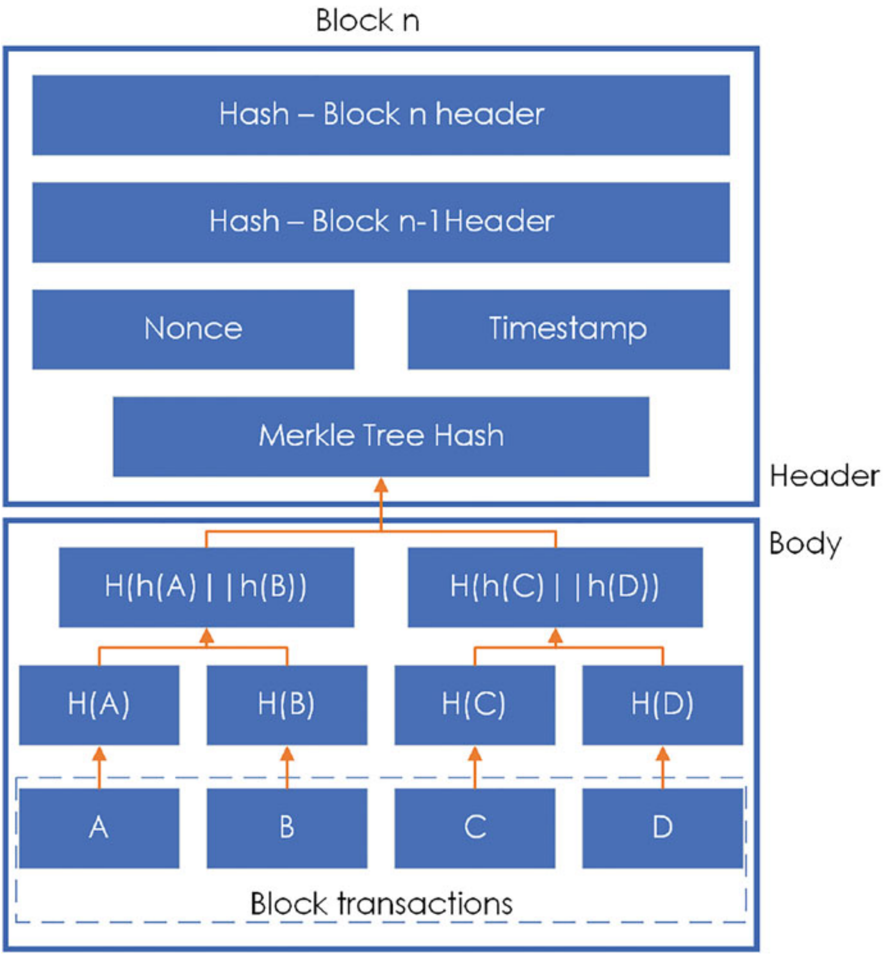


Fig. 4 Blockchain structure block [20]

3 Smart Contracts

The term ‘smart contract’ was defined by the programmer and cryptographer Nick Szabo in 1994 as *‘a set of promises, specified in digital form, including protocols within which the parties perform on the other promises’*. Basically, it is a program that, using all decentralised and tamper-resistant features of blockchain, allows the execution of several embedded codes over the blockchain. This code, designed specifically to store or calculate several values like a regular coding program, keeps immutable inside a block, where any modification requires the mandatory creation of a new block in the blockchain, with the references to the modified smart contract [21, 22].

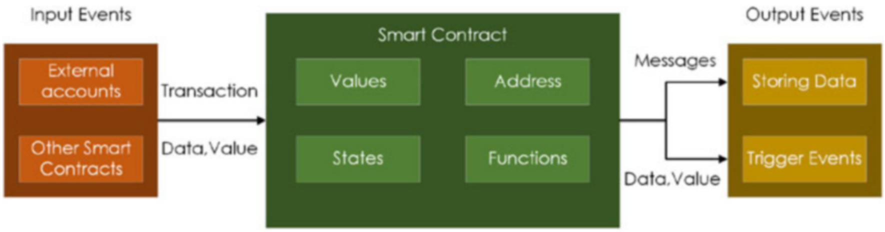


Fig. 5 Smart contract basic structure [22]

As a portion of code running over the blockchain, it is based on transactions made by the users or other smart contracts stored in the blockchain. Figure 5 shows a basic functional structure of a smart contract. As any other computational program, it depends on some inputs that can come from some external registered users (as non-node accounts) or from other smart contract information in the form of data/value pair. That is the information that triggers the execution of the smart contract. In general, every smart contract has four main components: (a) values, which update the fields of the smart contract, (b) state, which is the final state of the execution of the smart contract before its storage in the blockchain, (c) address, which is the address of the smart contract inside the blockchain and the update chain for every new smart contract based on the first-linked and (d) functions, which are the actual code executed when the smart contract is invoked and fed with the data, value pair. The output of the code execution inside the smart contract is also a data, value pair. The difference is the output that generates the storage of data inside the smart contract or the triggering of varied events defined in the smart contract functions. After all the execution, the final output is stored inside the blockchain and its result becomes immutable. These results can be modified in a new linked smart contract, with the same functions but with different address, data and states [22].

Every smart contract, as a part of blockchain, has all the properties of the ledger including the self-verification, tamper resistance and auditability over the whole transaction. That means that even when the transaction is secure, all the data are transparent for every user that utilises the specific blockchain. As blockchain itself, is not designed by default for data privacy.

Figure 6 shows how the process explained in Fig. 5 allows two parties to interact without a TTP. Both users A and B need to interact over some resources or assets, which are validated over the source code of the smart contract (there is a specific smart contract for every need of the network). This smart contract is designed to check if the parameters established for every transaction must be fulfilled before performing the transaction. Users A and B requirements are the input of the code and the information to be validated before confirming the transaction. If the terms and conditions of the smart contract and the input match, the transaction is considered valid and the smart contract is stored in the blockchain with the validation on the resources' interaction. If the input does not match the terms, the smart contract rejects the transaction and store the error message. As it is seen, there is no TTP

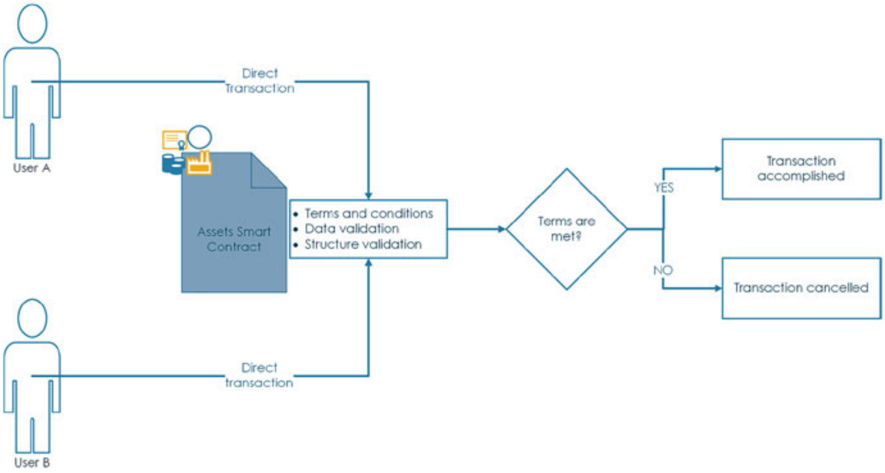


Fig. 6 Smart contract basic functioning

or external entity validating the transaction. A and B trust directly in the smart contract, implying that trust is placed in the algorithms and processes that conform the network, and not in its components.

4 Security Features

There are two considerations to explain all the security features of blockchain: infrastructure and transactions, regardless of the technology or type of blockchain being implemented. The following sections explain every one of these considerations and its features [10, 23].

4.1 Security on Infrastructure

The main security features of the blockchain infrastructure are as follows:

4.1.1 Decentralisation

The main characteristic of blockchain is to avoid by all means any centralised system or certification authority (CA), such as banks or government entities. Consensus protocols allow blockchain networks to achieve this main characteristic without any trustworthiness between the participant nodes. This paradigm also changes the network from the traditional client–server architecture and implements a decentralised network where all nodes have the same amount of information to provide to the network. All of this solves the very important security flaw of having a single point of failure, one that could be compromised, hijacked or misused.

4.1.2 Transparency

One of the main characteristics of any blockchain is to allow transactions to be carried out with any user without directly using their identity. All transactions are performed using encrypted and hashed addresses, which means that every identity remains private and anonymous. However, the transactions stored in the ledger are not private. The blockchain designed for Bitcoin, and all branches since it, were created to show all stored transactions, without any protection or cloaking algorithms. All users can verify all transactions at any time, but when the information stored is sensitive (such as identity information on a smart contract), transparency may be a security issue for some users or implementations.

4.1.3 Immutability

The information already stored in the ledger cannot be modified or altered without affecting all the following blocks. This is possible thanks to Merkle trees and hash functions, in particular the 'avalanche' effect of hashing. As illustrated in Fig. 3a, any change to a block, for example, Block b, after its confirmation and storage, will modify the whole following chain, creating, consequently, an illegal and unconfirmed branch. The ability of blockchain to store all data with an unbreakable security at all times is one of the most important features, not only in the financial field but also in all applications of Blockchain 3.0.

4.1.4 Consistency

This property refers to the ability of the network to have the same ledger in all registered nodes at the same time. The total consistency property differs among implementations due to the consensus algorithm used by each implementation. PoW provides less consistency than PoS or PoB because it depends on all nodes to agree on the longest chain. Small or back-to-back transactions are not a problem, but large transactions require a general agreement. This could open up three specific vulnerabilities (attacks), as described below:

DDoS Attack

This is a Distributed Denial of Service attack, where a large number of nodes execute a distributed flooding attack on the network. This attack can compromise the availability of the network, or part of it, to execute the PoW and gain access to the longest chain. The fully decentralised structure of the blockchain provides a countermeasure to this attack, but if an attacker is able to gather enough computing power on the network, he/she can effectively compromise larger portions of it, creating illegal branches of the blockchain that could masquerade as a longer chain [10].

Double-Spending Attacks

This refers to the ability of the entire network to make each transaction unique, so that the same transaction cannot be performed twice or that two different transactions will be performed with the same currency. Transaction inconsistencies are solved by the consensus algorithm, which is added to each transaction and is sent, signed by the creator. Consensus algorithms ensure that the consistency of the ledger is resistant to any malicious double-spending attack [8, 10].

Majority (51%) Attack

This is perhaps the most dangerous attack on consistency on the blockchain. The way blockchain is built makes it almost impossible to modify a branch or a specific block when it was consolidated in the chain. However, if a group of malicious attackers can impersonate or hijack at least 51% of the network computational power, the attackers can effectively modify the information in the blockchain. In fact, they will be able to create a fraudulent 'longest' chain or a new group of validators. Consensus protocols help in maintaining a single ledger because the majority of nodes confirm the longest chain or validators in the network. The success of this attack is inversely proportional to the size of the network, as it is almost impossible to control the 51% of a blockchain. Nevertheless, this is a security issue for any blockchain implementation [8, 23].

4.2 Security on Transactions

Blockchain transactions extend the infrastructure security because the ledger can also be considered as local network security between all nodes and entities that are part of the entire blockchain network. This means that the availability and integrity of each transaction can be maintained on any communication platform. This also includes the consistency and immutability of the entire network, which prevents double-spending and majority (51%) attacks. Transaction security relies on the decentralisation of each node and the anonymity of each user, making it impossible to track where or when transactions are generated or in which point the consensus is implemented.

The security of transactions can also be related to the anonymity and confidentiality of the transactions over the network, as it is explained in the following items [10]:

1. Every transaction in the blockchain, especially in Bitcoin, is anonymous (i.e. there is no identity information exchange during the transaction, only the wallet directions). However, as the transparency of the ledger grows, so does the ability to track the origins and destinations of almost every transaction stored in the ledger. The idea of unlinkability is to prevent the establishment of a relation between two or more users/nodes that are interacting in some transaction. This leads to understand that blockchain is based on a pseudo-anonymity to work. This can be seen as a vulnerability over de-anonymisation interference attacks (where attackers track the transactions to try obtaining the user's identity) [1].
2. Blockchain, as we know it, was designed to be fully transparent. With the creation of smart contracts over blockchain, we have also seen the appearance of several concepts of data privacy and confidentiality. That is because smart contracts can handle and implement more complex transactions than only-cryptocurrency exchanges. Based on this, smart contracts implement several security features that guarantee the privacy of not only the data but also the code of every smart contract and of the miner/validator that executes the contract and stores it into the blockchain.

5 Applications

The definitions of Blockchain 1.0 (only for cryptocurrencies) and 2.0 (limited smart contracts) made blockchain technology a new curiosity with important but limited applications. With the advent of Blockchain 3.0 (extended smart contracts), several new implementations of blockchain have emerged and are aimed to diversify the application of the decentralised ledger. The authors of [3] summarise six main applications of blockchain as a part of the 'hype' of the technology and not related to cryptocurrencies:

5.1 Electronic Voting

One of the 'natural' implementations of blockchain is the storage of voting ballots in political elections. The study of the electronic voting as the replacement of voting must be differentiated from polls or other informal voting systems. Based primarily on Ethereum and BallotChain, the main idea of this application is to create a decentralised system that stores ballots without the involvement of third parties for validation and presentation of results. The main features of this implementation are based on (a) the possibility of remote voting, where *users can use their devices to vote with a secure channel verifiable from end to end, where anonymity is well* *needed* and (b) the auditability of the system, *to verify that the system is tamper-proof in each node and maintain the anonymity of voters at each stage of the voting system.* All of this means that the blockchain can guarantee that no information will be altered, leaked or lost during the election process.

In a way, electronic ballots and cryptocurrency have some similarities in their concepts because both share the 'double spending' problem. A user can neither vote twice in the same election nor can a user spend the same amount of cryptocurrency twice. Also, both results must be public and auditable (the vote and the currency transaction), but the identity of the owner of the transaction must remain private and secure. To define better the idea of voting, the researchers have divided it into three phases: the registration of the voters, the vote casting and the result of the vote process. The registration is very important because define not only the addresses of every user but the addresses of every candidate as well, so the voters can cast their votes in specific addresses corresponding to every candidate in the process. The voting process is performed with voting tokens stored by users at the addresses of their chosen candidates, ensuring that users can spend that token only once for each candidate's address, and without exceeding the possible number of eligible voters (invalid voting processes would occur when a user submits more voting tokens than he/she is authorised to, if such a function is available in the system). The third phase consists of counting how many tokens each candidate has. However, very simple, this scheme helps to show the advantages and challenges of electronic voting and how blockchain would help to implement a tamper-proof auditable system to implement an efficient and secure electronic vote system.

5.2 Healthcare Services

The first implementation of the concepts of Blockchain 3.0, and the first one designed to solve a problem of users' personal information, in this case, healthcare personal data. With every medical procedure, a user generate an important amount of sensitive information which is currently 'owned' by healthcare services (doctors, pharmacies, insurance services and so on), making it difficult to share between services, and the user cannot know how much of their information is in fact held by health schemes. Efforts are currently underway to create a single transferable medical information scheme, called Electronic Health Record (EHR), where all user information can be stored in a consolidated in a single exportable format. In that way a patient, regardless of their country of origin or residence, can access to a reliable health service. However, patients still do not own the information stored in the EHR. With blockchain, the health information of every user can be stored in the networks in a decentralised way, so that although doctors are able to access and modify patient information, the ownership of the information remains with the smart contract, i.e. it belongs directly to the user.

This concept, while decentralising information and keeping it with its owner, presents two major problems in its implementation. First of all, and as it was seen in Sect. 3, all the information stored in a smart contract is public, meaning that any user of the network can access the information, although without modification permissions. Personal health information must remain private for every party, except the patient and his/her medical doctor. So, the challenge is having all the information of the user not only secure but also private. The amount of stored information resulting from the medical records of a lifetime is another problem for the implementation of a healthcare blockchain, not only in the amount of memory needed to store all the data but also because of the processing time of this large amount of information on the part of the medical provider.

This second problem nowadays has been solved by keeping information off-chain (in the traditional way) and using blockchain only for hashes and references, which is a temporary solution for the problem, but the transparency problem is still an issue for the wide implementation of a universal blockchain (or set of blockchains) for health data, according to the researchers.

5.3 Identity Management

Directly related to healthcare systems, identity management with blockchain aims to create a user-centric system where everyone's identity can be secure and cross-functional for any entity. The main feature of this implementation is that the user should have control of his identity, with full access to all its data. This eliminates malicious claims of identities, and hence, identity theft can be minimised. Moreover, decentralised systems must maintain the persistence and transparency of typical blockchain implementations to secure the user identity information, as is shown in [24, 25].

In order to keep the decentralisation scheme and the security needed by the user identities managed by a blockchain, it is important to consider how it must be done the management of the identity inside the network. To avoid any TTP, the users must have full control and access to their identities, meaning that the modification of stored information is the prerogative of the user, without any intermediary. Also, the system must assure the existence of the stored identity (no one except the owner can deregister its own identity), and also only the owner can provide the agreement in the use of his/her identity. In the same idea, every identity must be portable (interchangeable between analogue systems) and must be persistent (the storage of the identity must be able to be preserved over time), and the rights of every identity owner must be protected. Finally, the network itself must provide the algorithms to keep the network transparent [26].

Even though these features must be implemented in the identity management networks, it still remains the problem of healthcare systems: the amount of information stored could compromise the storage systems of the network and all this information is stored publicly. Additionally, the decentralisation of the identity managers implies new and different ways to interact with the identity requesters, which could lead to security breaches, not because of the network itself but because of the inexperience that users may have with it.

5.4 Access Control

The information security management theory explains how the assets must be stored in secure facilities, where only the users with a specific clearance can access. The main idea of using a smart contract to implement a new access control system is to replace the traditional logs of people and devices with specific blockchain-based ones when the interaction is with systems such as IoT recordings or corporate access control logs. The policies about access control, like request of permissions, authorisations or revocation of permissions, will be stored for each user interaction with the respective smart contract, leaving a transparent log available for any kind of audit. In addition, as the result of the smart contract execution cannot be forged easily, the result of the access control transaction can also be used as a part of the physical access control and not only as the enforcement of the access policy. Blockchain technology offers to minimise the computational time to store and keep immutable the access log that can be directly audited and controlled. Although this system offers transparent logging, it can still be vulnerable by making too much information available to all users, potentially creating a privacy problem within the access control scheme.

5.5 Decentralised Notaries

The cryptographic suite of the blockchain (primarily the hash functions) allows the ledger to be used as a decentralised trust witness that can verify and certify agreements between mutually untrustworthy parties, using the blockchain as a replacement of the trusted third party, which means achieving the same level of trust without relying on a TTP. By keeping every agreement stored in the ledger, each party has the security of any agreement that was made, and any non-compliance issues can be probed without relying on a TTP.

The most important feature to consider is the validation of timestamps when the information to be validated is stored on the blockchain. It means the decentralised notary must be able to prove that in one point of time, the stored information existed. Or, if the information stored is a hash or a digest of a document, that hash proves that the information was untampered when the consensus finishes the creation of the block. The proof of hashing is known as proof of ownership because it is based on the concept that only the owner of the document could have generated the hash that allows validation by making a positive comparison between the hash of the document (physical or digital) and the hash stored in the blockchain.

The main application of decentralised notaries is the validation of existence and ownership of digital contents in the context of intellectual property claims. The smart contracts could be programmed to analyse the timestamps in a chain of contracts to validate that the owner effectively owns the digital asset. In the same idea, the smart contract can allow other users to consume the digital asset (for example, a portion of licenced code or a song) if those users have 'purchased' the rights to do it. All of that increasing the transparency of the intellectual property claims while reducing the energy consumption and eliminating the intermediaries between an owner and the costumer.

5.6 Supply Chain Management

The agreement on the creation of a product or service based on natural resources uses blockchain as a tool that allows guaranteeing the auditability and transparency of each process, without spending a lot of resources between mutually untrustworthy parties. The resources can include human intellect, certifications, legal standards and regulations, all of which can be stored on a specific smart contract, without the need for an impartial witness (a notary) to validate the production and specification of a particular product or service.

In Sect. 5.5, it is presented a system that provides a timestamped proof of ownership and the existence of a digital asset through smart contracts. With the same idea, the record of creation of an asset, from the acquisition of its raw production material through all the transport and product validation schemes to its arrival at the final consumer, can be validated at each inspection point, verifying (through the smart contract parameters) that all preestablished agreements for the given asset have been fulfilled. In this case, the asset is a physical product and all its transport process. In order to improve the traditional supply chains, the decentralised system must increase the transparency over every asset, which is fulfilled by transparency of the smart contract and the traceability of all changes made on the asset by the producer or by those responsible for transport and handling. Both transparency and traceability help to keep an easier auditability of every asset without the traditional inspections. With that, the cost and speed of management and verification of every product in the supply chain will be improved, by eliminating several middlemen and other parties that helped to maintain the established parameters of production but slowed down the creation and transport of products.

Figure 7 shows the full supply chain for a product and what is the information that must need to be stored in every iteration of the smart contract, from the factory to the costumer store. Every raw material producer (1) needs to certificate the data of origin and processing of its materials before the correspondent packaging. When the materials are packaged, every package must certificate the shipment information, and the order over which those products are packaged (2). With all this information, the materials are stored in a main storage facility, where the data of origin, processing and transport are validated for the first time (3). The smart

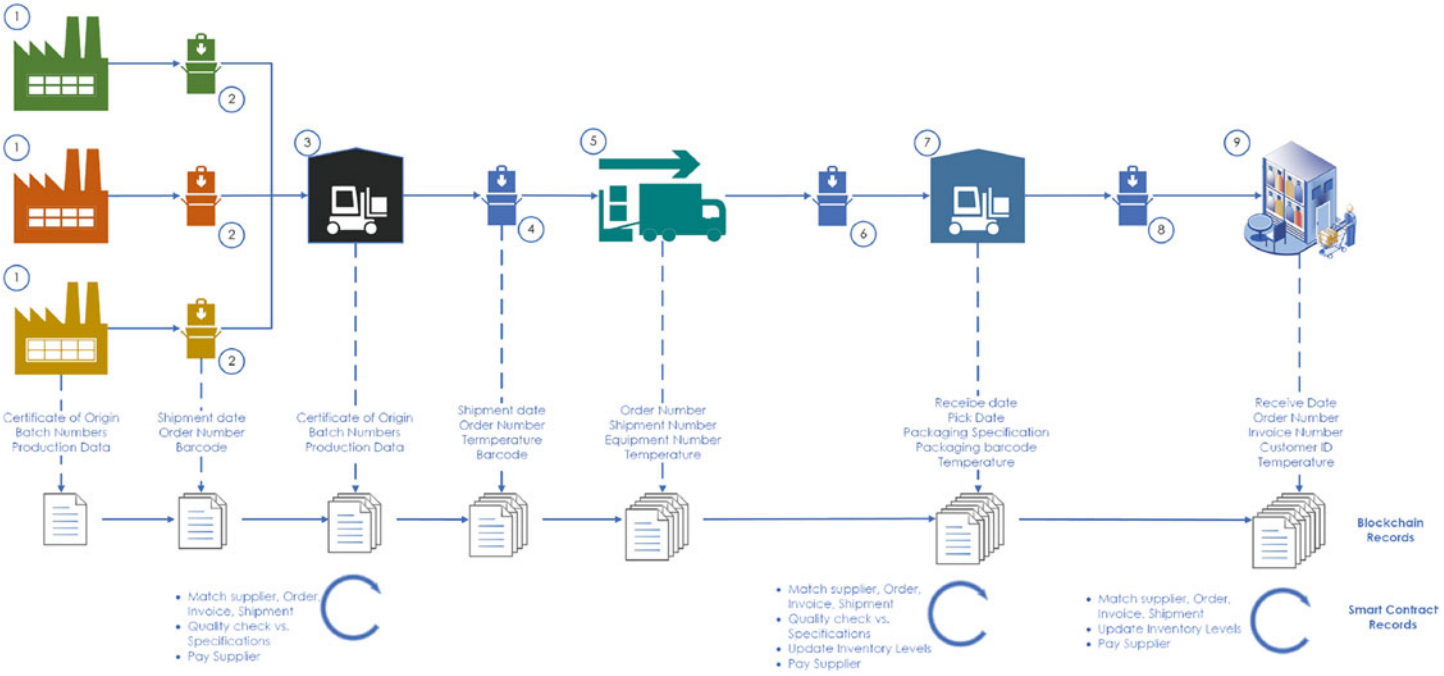


Fig. 7 Supply chain management system though blockchain records [27]

contracts of every raw material are validated and updated for the storage facility system in order to check whether the raw material complies with the parameters according to which it was created and/or requested for transport. After this first validation, the materials are packaged again for shipping (4), grouping them already according to their final destinations. For this first shipping (4), the system must validate the dates and the order numbers, to validate the origin of the shipment, and also all the features of the transported product, like temperature or packaging. When the shipment is transported (5), every order number must be validated to redirect all the shipments to their correct destinations, in such a way that there is no confusion between the packages in transport (6 and 8). In the intermediate storage facility (7), the information of order numbers, production and delivery dates and all the packaging specifications are checked again before the shipment continues to the final destination. For this example, the costumer store (9) is the final destination, where the final seller needs to check again all the dates and order numbers, and also if the conditions of the received product matches with the stored in the smart contract, completing the whole process [27].

With this process based on decentralised supply chains, validation processes that can currently take weeks are completed in a few days, and the end user has the certainty that there were no errors or failures during the transportation of their product, because given the security of blockchain, the validation information cannot be modified or tampered by rogue parties during the shipment.

6 Conclusion and Future Works

The appearance of Bitcoin and its corresponding blockchain, opened up a new perspective on information management in open environments, not because of the new technology presented or the novelty of its possible applications, explained in this chapter, in Sect. 5, but because it changed the paradigm of application management to a version where the user and the control of his or her data allowed the network to exchange information. We moved from a network based on large data managers (servers) to a network based entirely on the user and the relationships he or she could establish between peers. It was the origin of the user-centric network [1].

Since then, this new paradigm leads to the creation of new ways to understand decentralisation and also how complicated it is in front of a simpler but centralised network, where all the services are concentrated. Blockchain is an emerging technology which could lead to a revolution in the way of how we understand the network and how we can improve our own interactions not only with the network itself but also with other real-world applications, where blockchain is actually an improver of every function and implementation. However, it is important to understand not only the benefits of the technology but also their limitations and improvements. In this way, blockchain can become a tool that allows the development of secure interactions between users and that users feel comfortable interacting with a blockchain; without thinking that the technology is the solution to all the problems of the Internet.

The future developments of blockchain include several perspectives over its functioning and implementation. One of the big challenges of the decentralised applications is to find efficient ways to handle the information from both perspectives: (a) the security and privacy of the data, because as it was explained, blockchain allows the store of information in such a way that it is almost impossible to modify it. All of this information, however, is public and transparent, creating a privacy issue, especially in applications where the information stored corresponds to the identities of the users. (b) The energy consumption to keep the network working. Consensus protocols as PoW achieving the full decentralisation and anonymity in the creation of the new blocks, but with a high energy consumption, which is an environmental issue nowadays. The consensus based on stakes, like PoS or PoC, are more energy efficient but ignore the decentralisation in the creation of the new blocks, which could lead to the hijacking of the network by resourceful rogue parties, like in OpenPGP [28].

Another challenge in the evolution of blockchain relates not so much to technical improvements to the system but to its use within a decentralised network. In Sect. 5, it is explained how the current blockchains allow the improvement of systems where the information storage and the chain of procedures are the main examples. However, the storage of information, offline or online, can be part of new security developments where the time immutability is critical. It means using the tamper-proof of blockchain to store information that it not only remains unchanged from present changes but also maintains its form and codification for future revisions, especially on issues of encryption and encryption of information and the ability to keep information encrypted and secure regardless of when cryptographic suites are modified in the future. All of these features can lead to a secure-by-design network where all the information can be decentralised and remain secure in a future where, with quantum cryptography in the near horizon, we do not really know how much of our current security can remain functional and with that how much of our now secure information can retain that feature. The future improvements of blockchain can lead us to a new way to understand network itself and all of our relation with it.

References

1. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Rev., 21260 (2008)
2. A. Narayanan, J. Clark, Bitcoin's academic pedigree. Commun. ACM **60**(12), 36–45 (2017)
3. D. Di Francesco Maesa, P. Mori, Blockchain 3.0 applications survey. J. Parall. Distributed Comput. **138**, 99–114 (2020)
4. G. Wood, Ethereum: a secure d generalized transaction ledger. Ethereum Project Yellow Paper **151**, 1–32 (2018)
5. N. El Madhoun, J.Hatin, E. Bertin, A decision tree for building it applications. Ann. Telecommun. **76**(3), 131–144 (2021)

6. Z. Wan, R.H. Deng, D. Lee, Electronic contract signing without using trusted third party, in *International Conference on Network and System Security* (Springer, Berlin, 2015), pp. 386–394
7. S. Zaid, G. Linscott, A. Becevello, T. Zaid, P. Lem, System and method for anonymous addressing of content on network peers and for private peer-to-peer file sharing, US Patent 9,112,875, 2015
8. X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
9. Y. Caseau, S. Soudoplatoff, *La blockchain, ou la confiance distribuée*. (Fondation pour l'innovation politique, Paris, 2016)
10. R. Zhang, R. Xue, L. Liu, Security and privacy on blockchain. ACM Comput. Surv. **52**(3), 1–34 (2019)
11. L.S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of consensus protocols on blockchain applications, in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)* (2017), pp. 1–5
12. M. Ahmed, I. Elahi, M. Abrar, U. Aslam, I. Khalid, M.A. Habib, Understanding blockchain, in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems - ICFNDS '19* (2019), pp. 1–8
13. E. Muzzy, What Is Proof of Stake? | ConsenSys (2020). https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/. Retrieved: 07 May 2021
14. K. Karantias, A. Kiayias, D. Zindros, Proof-of-burn, in ed. by J. Bonneau, N. Heninger, *Financial Cryptography and Data Security* (Springer International Publishing, Berlin, 2020), pp. 523–540
15. Slimcoin: Slimcoin Project (2014). https://github.com/slimcoin-project/Slimcoin/. Retrieved 28 march 2022
16. S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, SoK: Consensus in the age of blockchains, in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*. AFT '19 (Association for Computing Machinery, New York, 2019), pp. 183–198
17. S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak, Proofs of space, in ed,. by R. Gennaro, M. Robshaw, *Advances in Cryptology – CRYPTO 2015* (Springer, Berlin, 2015). pp. 585–605
18. S. Park, A. Kwon, G. Fuchsbauer, P. Gaži,, J. Alwen, K. Pietrzak, SpaceMint: A cryptocurrency based on proofs of space, in ed. by S. Meiklejohn, K. Sako, *Financial Cryptography and Data Security*. Lecture Notes in Computer Science, vol. 10957 (Springer, Berlin, 2018), pp. 480–499
19. Sawtooth: Hyperledger Sawtooth (2016). https://github.com/hyperledger/sawtooth-core. Retrieved 28 March 2022
20. L. Axon, Privacy-awareness in blockchain-based PKI. CDT Tech. Paper Ser. **21**, 15 (2015)
21. A.M. Antonopoulos, G. Wood, *Mastering Ethereum*, 1st edn. (O'Reilly Media, Sebastopol, 2018)
22. B.K. Mohanta, S.S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (2018), pp. 1–4
23. I.C. Lin, T.C. Liao, A survey of blockchain security issues and challenges. Int. J. Netw. Secur. **19**(5), 653–659 (2017)
24. D. Maldonado-Ruiz, J. Torres, N. El Madhoun, M. Badra, An innovative and decentralized identity framework based on blockchain technology, in *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (2021), pp. 1–8
25. B. Hammi, S. Zeadally, Y.C.E. Adja, M.D. Giudice, J. Nebhen, Blockchain-based solution for detecting and preventing fake check scams. IEEE Trans. Eng. Manag. 1–16 (2021)
26. A. Tobin, D. Reed, The inevitable rise of self-sovereign identity. Sovrin Found. **29**, 18 (2016)
27. Resolve: Blockchains for supply chains – part II (2016). https://resolvesp.com/blockchains-supply-chains-part-ii/. Retrieved 28 March 2022
28. D. Maldonado-Ruiz, E. Loza-Aguirre, J. Torres, A proposal for an improved distributed architecture for OpenPGP's web of trust, in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)* (2018), pp. 77–81

Identification of Illicit Blockchain Transactions Using Hyperparameters Auto-tuning

Enrico Zanardo, Gian Pio Domiziani, Elias Iosif, and Klitos Christodoulou

1 Introduction

In a blockchain framework, individuals are able to exchange generic form of chunk of data through a distributed peer-to-peer (P2P) network. Such distributed P2P is established by the peers following the given protocol. The validity of each transaction in terms of ownership and correctness is entrusted by the network itself, in a distributed way without the necessity of a trusted third part. In a sense, the trusted third part's role is played by the distributed peers, following a particular consensus protocol. However, even if the used consensus protocol assures reliability for each transaction, it is unknown to users if the addresses with which they have exchanged content deserve trust or not because the identity of such address may be unknown.

For instance, in the Bitcoin ecosystem, each wallet has its own address (public key), and other wallets (users) can exchange transactions, with it sending forward that address, without the necessity to know who is behind that address. This means that anyone can exchange bitcoin transactions without directly public reveal his/her identity [7]. Such possibility has already opened serious legal problems, as money laundering, ransomware demands, and the purchase of contraband goods and services [18].

In particular, Bitcoin seems to be the most widely used cryptocurrency exploited for criminal activity, where ransomware victims are pressed to exchange the ransom

E. Zanardo (✉) · E. Iosif · K. Christodoulou
Dept. of Digital Innovation, School of Business & Institute For the Future, University of Nicosia, Nicosia, Cyprus
e-mail: zanardo.e@live.unic.ac.cy; iosif.e@unic.ac.cy; christodoulou.kl@unic.ac.cy

G. P. Domiziani
OneZeroBinary LTD, San Pawl il-Baħar, Malta
e-mail: gpdomiziani@onezerobinary.com

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_2

from fiat currency to Bitcoin and transfer this amount to a specific Bitcoin address that is provided by the criminals. Again, on underground markets, large amounts of goods and services—like drugs, weapons, and DDoS attacks—are bought and sold using Bitcoin as method of payment [14].

Mixing services enable the "masking" of initial transactions by assigning new addresses to the sender and receiver, such that to making the transaction tracing difficult. Note that even if the address is not associated with a real identity, it could be associated with an IP, allowing the detection of the respective identity. The Spring of 2020, the Cryptocurrency Crime, and Anti-Money Laundering report from blockchain intelligence and forensics company CipherTrace[1] revealed the global amount of Bitcoin crime attributed to fraud and misappropriation as USD 4.5 billion in 2019. A high proportion of these illicit Bitcoin transactions (74%) moved from exchange to exchange across jurisdictional borders. The report argues that the nature of these "cross-border" transactions emphasizes the need for cryptocurrency exchanges to adopt and ensure appropriate compliance. Also, the report underlines how the global average of direct criminal funds received by exchanges dropped 60% from 2017 to 2019, most of which occurred in the last year with a 47% drop from 2018 to 2019. This trend marks a three-year low for cryptocurrency exchanges around the world, with an average of only 0.17% of funds received by exchanges in 2019 coming directly from criminal sources.

Luckily, the very nature of the blockchain implies that each transaction is hashed in a distributed ledger, without the possibility to be changed. That feature assures that data exchanged assume an immutable version. First of all, that characteristic implies that in a blockchain system it is not possible to build adversarial attacks such as those described in [2], since the architecture of the transactions graph cannot be modified. Second, it could be possible to investigate the transaction graph in order to underline illicit behavior associated with a given address [1, 9, 11, 17, 21].

The prevention of fraud transactions becomes of absolute importance for all the financial related activities, which could be done through blockchain frameworks. The entire credibility of potential fintech blockchain applications relies on the robustness and resilience against cybercrimes. Furthermore, the proposed methods must be precise, ensuring that the number of false positives is as low as possible, as well as inclusive, allowing for a lower number of false negatives, preventing honest addresses from being classified as illicit.

Motivated by the above considerations, this work proposes a new approach for improving the robustness of machine learning algorithms for classifying Bitcoin transactions as *licit vs. illicit*. Our approach relies on a well-established dataset, while the proposed method improves the performance (precision, recall, F1, and micro-F1). Furthermore, the respective source code is made publicly available.

[1] https://tinyurl.com/3xpcsb6w.

2 Related Work

Several computational models have been used in the area of blockchain including the estimation of blockchain-related business intelligence such as blockchain readiness [4], utilizing techniques from other disciplines like unsupervised machine learning on semantic similarity, e.g., [3], and web mining, e.g., [5]. A broad category of those models deals with the dynamics of the network including the computation of analytics both at the user and at the transaction level. Regarding the employment of computational approaches for identity exploration, one of the first attempts was presented in [13] focusing on the analysis of Bitcoin blockchain to reveal identities. The heuristics applied in this work form the basis upon which today's Bitcoin analysis is performed. These heuristics make it possible to cluster activity around a certain user and add context to this user for purposes of identification or grouping similar services on the network. In addition, it introduces the concept of peeling, where smaller amounts of Bitcoin are "peeled" off a larger amount and transferred onto another address with the remainder transferred back to the one-off change address.

In [9], a methodology was suggested for predicting the BTC price fluctuations utilizing an inverse reinforcement learning (IRL) and an agent-based modelling method (ABM). Rather than estimating relationships between price-related factors and market pricing, the approach consisted of forecasting prices by reproducing synthetic behavior of agents in simulated markets. The IRL model provided a method for finding the behavior rules of agents from blockchain data in an orderly manner by framing trading behavior as a barrier to rectifying the motivations of known behavior and issuing guidelines that are consistent with the observed motivations. Once the rules/guidelines are corrected, the agent-based model generates hypothetical relationships between observed behavior rules, resulting in an equilibrium price as emergent characteristics by matching Bitcoin demand and supply dynamics. ABM, on the other hand, demonstrated that manually created individual rules/guidelines were the result of IRL-channeled ones. The experimental results showed that the proposed method can forecast market prices in the short term as well as outline overall market trends.

In [17], the authors investigated the question: "Given an address, is it possible to classify it as belonging to a particular services or purpose?" In this framework, seven different services were considered: exchange/wallet, faucet, gambling, HYIP, marketplace, mining pool, and mixer. The authors adopted a multi-class problem, that is, the classification of an address to one of those services. This was conducted by exploring the transaction history, using a supervised machine learning approach. The history of transactions was built by the following two schemes: (1) Address-based and (2) Owner-based schemes In the address-based scheme, when a Bitcoin address is given, any transactions where it is involved either in the inputs or in the outputs are retrieved and the wanted features are extracted. In the owner-based scheme, thanks to the help of address clustering, other addresses controlled by its owner are also extracted. Using a dataset including 1360 owners and 26,313 Bitcoin address, this study reached 70 and 72% of accuracy for the owner-based scheme and the author-based scheme, respectively. In [10], the same multi-class classification task was studied, using a similar supervised learning scheme and starting by the same dataset used in [17]. However, in [10], a richer set of features was utilized, using extra statistics, with the objective of modelling temporal relations between transactions. The obtained performance was reported to be 87 and 86% for Micro-F1 and Macro-F2, respectively, using the LightGBM classifier.

In [21], the authors proposed a supervised learning model for classifying a given transaction as *licit* or *illicit*, in order to have a level of risk of a given transaction to/from cryptocurrency wallets. The dataset used maps Bitcoin transactions to real-world entities that fall into the licit and illicit categories, for example, {exchanges, wallet providers, miners, etc.} vs. {ransomware, Ponzi schemes, etc.}). A graph is constructed from the raw data, with nodes representing Bitcoin transactions and edges representing the flow of Bitcoin currency (BTC) from one transaction (node) to the next. If the user initiating the transaction (i.e., the entity owner of the private keys associated with the transaction's input addresses) falls into the licit (illicit) category, the transaction is labeled as "licit" (otherwise, "illicit"). In total, there is a total of 203,769 node transactions. The top performing model, Random Forest, was reported to achieve 0.796 F1 score. Further information about the dataset constructed a part of the study presented in [21] is provided in the section that follows.

3 Experimental Dataset

In the present work, we have used the dataset developed in [21], *Elliptic dataset*. Also, we have extended the respective machine learning approach that exploits this dataset. The Elliptic constitutes one of the largest publicly available labeled dataset, in any cryptocurrency, dealing with the licit/illicit characterization of transactions. In the next paragraphs, a summary of the dataset is provided.

The dataset consists of three documents:

- Class document: each transaction ID has one of the three possible classes (labels), namely, licit, illicit, and unknown.
- Edges document: this document defines the edges of the graph. An edge exists between transaction IDs.
- Features document: it defines a set of features for each transaction.

The distribution of the aforementioned classes in the dataset is as follows: 21% licit, 2% illicit, and 77% unknown.

Another observation is that the authors of the dataset do not determine how the features were engineered. Also, a series of heuristics were followed. For instance, a higher number of inputs with the reuse of same address were mapped to the same entity in the Bitcoin blockchain. Also, users following a low number of addresses were more likely to be characterized as illicit.

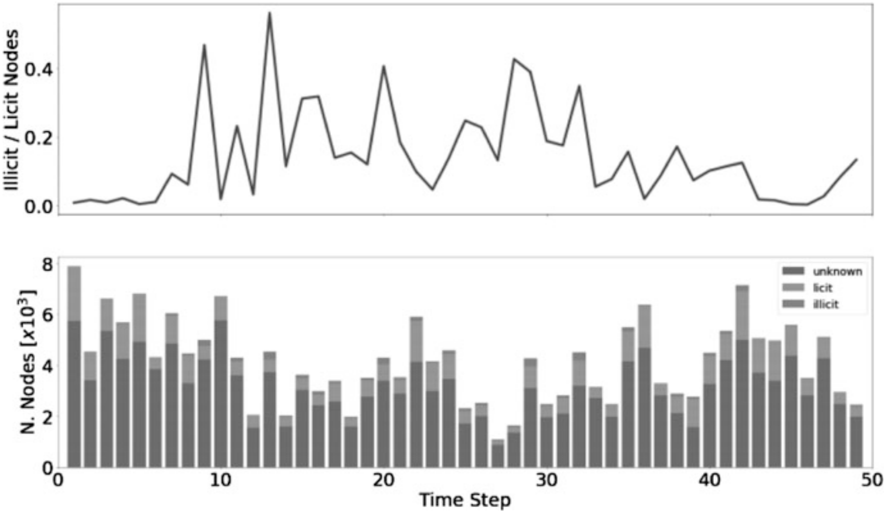


Fig. 1 Licit and illicit labels as a function of time step

As depicted in Fig. 1, each transaction has a time step associated with it, which indicates when the transaction was confirmed. A time step is made up of a single linked component of transactions that were settled within 3 hours of each other or less. In the Elliptic dataset, there are 49 time steps in total, evenly distributed over about 2 weeks. Every transaction has 166 attributes that are divided into two categories: local and aggregated features. Features such as transaction fee, the number of outputs/inputs, and time step are among the first 94 attributes (local features). The other 72 attributes include aggregated information extracted for local features (e.g., transaction fee and inputs/outputs) from one hop backward/forward from the central vertex, such as the standard deviation and correlation coefficients of neighboring transactions [21].

4 Experimental Setup and Evaluation

This section presents the experimental setup followed by the evaluation of the scenarios we have adopted, namely, *offline* and *online* learning. Four classifiers have been employed: Linear Regression (LR), XGBoost(XGB), Random Forest(RF), and LightGBM (LGB) [6].

The first scenario (offline learning) consists of a train/validation phase that employs cross-validation with a varying number of folds and a final evaluation phase in which the used model classifies a batch of previously unseen samples. As illustrated in Table 1, the `CV` parameter defines the number of folds to be used in the train. `Class weight` is a Boolean flag indicating the balancing of the

Table 1 Parameters

NAME	VALUE
CLASS_WEIGHTS	[False, True]
CLFs	[lgbm, rf, lr, xgboost]
CVs	[5, 10, 15]
LAST_TIMESTEP	49
LAST_TRAIN_TIMESTEP	34
SEED	456

labels. `CLFs` is the list of classifiers, where `LAST_TRAIN_TIMESTEP` is the range defining the train window (from the 0 time step to `LAST_TRAIN_TIMESTEP`), `LAST_TIMESTEP`, `LAST_TRAIN_TIMESTEP` are representing the test window. Finally, `SEED` is fixed for re-producibility. As a result, the initial dataset is divided into train and test datasets, with the train being further divided into a second train/validation dataset and the test being used for the evaluation phase.

In the second scenario (online learning), the classifier is given a fixed sample size for training and is asked to predict a smaller sample size in real time, after which the training dataset is expanded with the last prediction plus the starting samples. This method enables the lookup of all the available samples in a uniform manner, based on the prediction made for each time step.

Each offline experiment is composed of two distinct parts/phases. The first one, where the parameters reported in Table 1, are executed in a loop cycle, and at each iteration, the selected classifier, *clf*, is instantiated with the scikit-learn [15] default parameters. Then, the best two classifiers, in terms of `F1 score`, are selected and an *auto-tuning* phase is performed, by making use of the open-source library `FLAML` [20].

The online experiment is executed using the two selected best classifiers, where the optimal parameters, as obtained by the optimal search algorithm, are used. For each experiment, given the unbalanced dataset, in addition to the `F1 score`, the `Micro F1 average score` is also reported, along with the associated precision and recall scores.

4.1 Offline Learning

In the offline experiment, the parameters reported in Table 1 are tuned, in a loop, where for each iteration an instance of the selected classifier is created.

In Table 2, the best result of the first phase, with the above selected parameters, is reported. In terms of `F1 score` and the `Micro F1`, the two best performing classifiers are LightGBM and RF, with the default configurations as reported in the `scikit-learn package` [15].

The evaluation results for all classifiers are depicted in Fig. 2 for a specific number of time steps. It is observed that `LR` reaches the worst results, while

Table 2 Offline results

	LR	XGB	RF	LGB
Precision	0.327	0.813	0.917	0.854
Recall	0.707	0.723	0.717	0.729
Micro-F1	0.886	0.913	0.977	0.974
F1	0.447	0.765	0.805	0.786

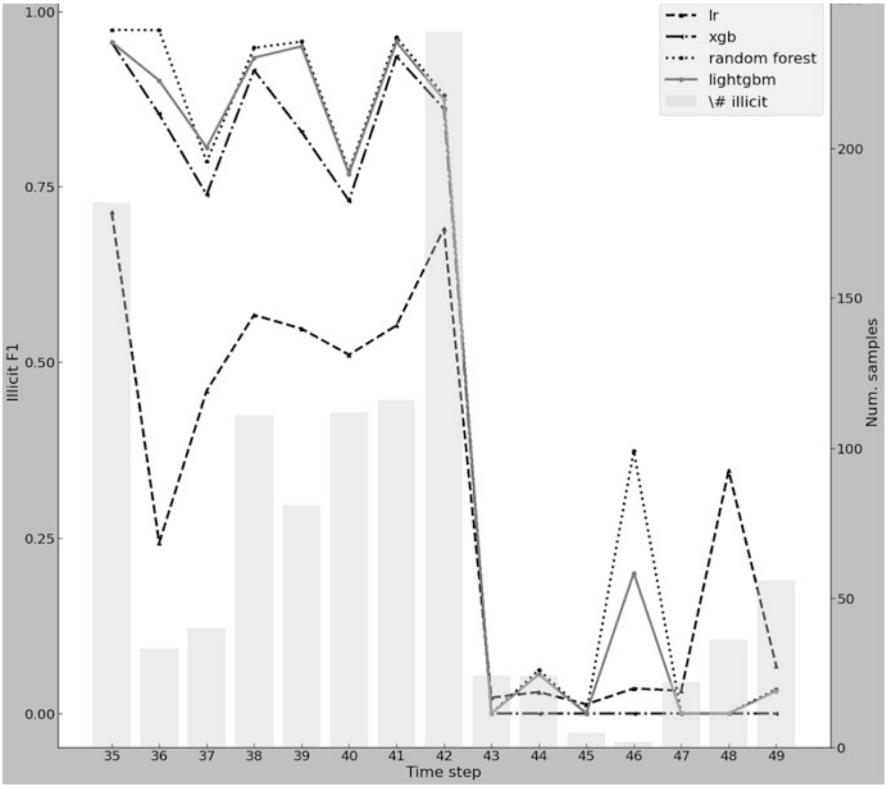


Fig. 2 Evaluation results for all classifiers

XGBOOST is not able to provide any valid results from the 43 to the final time step. LGBM and RF follow more or less the same shape. Consequently, the XGBoost was excluded from successive explorations.

4.2 *Online Learning*

Auto-tuning Phase From the offline experiment, the two best classifiers are RF and LGB, reaching a F1 score of **0.805** and **0.786**, respectively. The auto-tuning

Table 3 Final values for parameters

LightGBM	Random forest
n estimators: 100	n estimators: 13
Num leaves: 17	Max features: 0.8730950943488909
Min child samples: 33	Criterion: entropy
Learning rate: 0.09438604883209972	
Subsample: 0.9336368694068224	
Colsample bytree: 0.49899338695396656	
Reg alpha: 0.037525442727811574	
Reg lambda: 1.2037412273658785	

was performed, for these two types of models. The `FLAML` open-source library has been tested. It is an open-source project,[2] in which it is possible to perform an auto-tuning based on some defined parameters (settings). In particular, `FLAML` makes use of two recent optimal hyperparameter search algorithms *BlendSearch* and *CFO* (Frugal Optimization for Cost-related Hyperparameters) [19, 22], both are based on the same randomized direct search methods algorithm $FLOW^2$, which, unlike the Bayesian Optimization, it try to construct a conditional probability distribution of the cost function. Given the configuration of the chosen hyperparameters (Bayes's rule)—we start with an initial configuration of the hyperparameters which returns a low cost of the objective function x_0 s.t. $g(x_0)$ is small (the cost), and we define a step (differential) δ, and at each iteration $k \in K$, we choose a vector of random hyperparameters x_k, and we compare $f(x_{k-1} + x_k \cdot \delta)$ with $f(x_{k-1})$, selecting as hyperparameters vector that which results in a smaller (or maximum depending on the min/max problem) value of the objective function. The two best configurations are reported in Table 3.

The online configuration experiment has been done, using the *optimal* parameters obtained in the auto-ML tuning phase. The experiment consists in using **70:30 ratio** size for **training and test/evaluation**. The training/validation phase is performed with time series split cross-validation, using a number of fivefolds, with a fixed size of validation data of 10% of the initial 70% of training data. Using that method allows to validate the model over all the time steps, except for the first 15 time steps, used in the first fold. The evaluation is performed, as before, for the time steps in the range [35, 49].

In Table 4, the average `F1` and `Micro F1` scores are reported, for the validation phase, where the LightGBM model reaches 0.907 of `average F1` scores over the fivefolds.

In Table 6, the evaluation results are reported: the `LightGBM`, best model, reaches an `F1 score` of 0.819, with an **improvement of 2.1% with respect of the default parameters, as well as with respect to the best results obtained in [21]**,

[2] https://github.com/microsoft/FLAML.

Table 4 Validation of average results over the fivefolds

	RF	LGB
AVG Micro-F1	0.972	0.978
AVG F1	0.885	0.907

Table 5 Confusion matrix for the LightGBM

0	**1.00**	**0.00**
1	**0.29**	**0.71**
	0	1

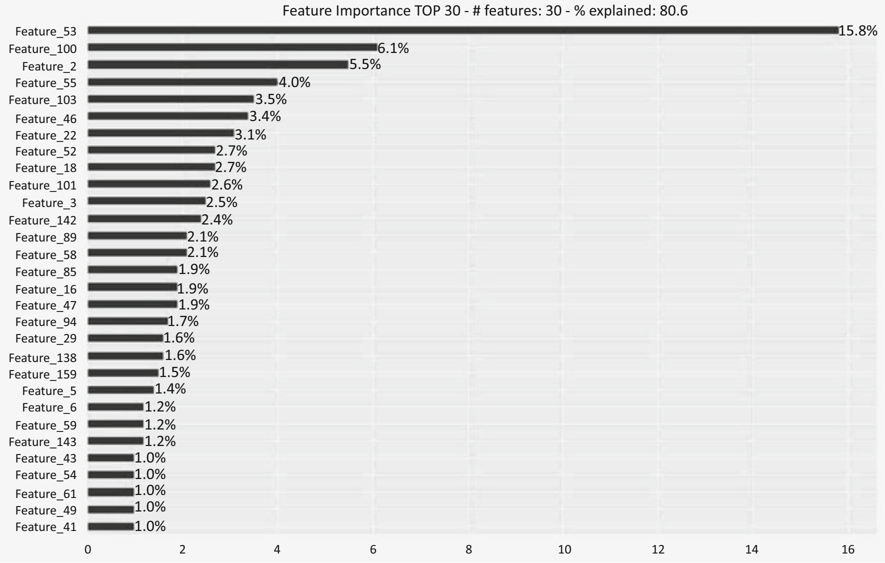


Fig. 3 Feature importance averaged over fivefolds

Table 6 Evaluation results

	RF	LGB
Precision	0.841	0.969
Recall	0.717	0.710
Micro-F1	0.974	0.980
F1	0.782	0.819

which is our main comparison target. The RF model does not reach an improvement with respect to the default parameters.

Continuing with the comparison, the LGB model reaches a close to zero number of False Negative, as shown in Table 5, therefore avoiding to classify licit transactions as illicit ones, assuring an inclusive predictive behavior. Figure 3 displays the 30 most significant aspects of the LGB model.

The obtained results are shown in Table 6.

Fig. 4 Percentage of explained variance as a function of number of features

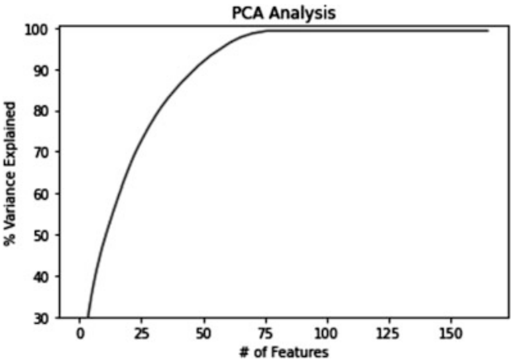


Table 7 PCA: evaluation results when using reduced number of features

	RF	LGB
Precision	0.869	0.947
Recall	0.128	0.426
Micro-F1	0.942	0.961
F1	0.224	0.587

4.3 PCA Analysis

Furthermore, a Principal Component Analysis [16] was performed, aiming to identify the minimum number of features needed for explaining at least 95% of the data. In Fig. 4 shows the percentage of variance explained as a function of the number of features. It is observed that 75 components can explain more than the 96% of data. Two experiments were performed, using a pipeline starting with the application of a PCA with a number of 75 and 85 features, using two best selected classifiers: RF and LGB. The results are presented in Table 7. The main observation is that this approach does not reach comparable results when compared to the full feature set, specifically, `F1` score of 0.587 for LGB and 0.224 for RF.

5 Conclusions

In this work, we have investigated `Elliptic Dataset` [21], an anonymous Bitcoin transactions dataset, composing of more than 170 features. The main aim was about trying to improve the performance of the machine learning model proposed by the creators of the dataset. This was conducted by employing an auto-tuning library.

The main achievement deals with the improvement of the `F1 score` for the LightGBM of 2%, making the model more robust against predicting false positive and false negative. Furthermore, PCA was performed, reporting a number of 75 features as optimal number of features, and however, the obtained results were not sufficient, in comparison with the results obtained using all features. This finding can be associated with the unbalanced character of the dataset. Indeed, less than the 2% of the transactions are labeled as illicit, meaning that the explained 96% of the data, as reported by the PCA Analysis, do not imply to be able to explain the illicit transactions.

As part of future work, it is needed to explore a statistical method for tackling the unbalanced character of the dataset. A first approach could be the use of a classical statistical method for that problem [8], as baseline, and then compare it with modern approaches such as [2, 12].

Last but not least, our contribution also includes the release of the source code[3] of this work, which has been made publicly available.

References

1. K. Christodoulou, E. Iosif, S. Louca, M. Themistocleous, Identity discovery in bitcoin blockchain: Leveraging transactions metadata via supervised learning, in *Proceedings of the 3rd International Conference on Vision, Image and Signal Processing* (2019), pp. 1–6
2. H. Dai, H. Li, T. Tian, X. Huang, L. Wang, J. Zhu, L. Song, Adversarial attack on graph structured data, in *International Conference on Machine Learning* PMLR (2018), pp. 1115–1124
3. E. Iosif, A. Potamianos, Similarity computation using semantic networks created from web-harvested data. Nat. Language Eng. **21**(1), 49–79 (2015)
4. E. Iosif, K. Christodoulou, A. Vlachos, Computation of blockchain readiness under partial information, in *European, Mediterranean, and Middle Eastern Conference on Information Systems* (Springer, Berlin, 2021), pp. 87–101
5. E. Iosif, K. Christodoulou, A. Vlachos, Web mining for estimating regulatory blockchain readiness (2021). Preprint arXiv:2103.13235
6. G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, T.Y. Liu, LightGBM: A highly efficient gradient boosting decision tree. Adv. Neur. Inf. Process. Syst. **30**, 3146–3154 (2017)
7. M.C.K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Commun. Surv. Tutor. **20**(3), 2543–2585 (2018)
8. B. Kitchenham, A procedure for analyzing unbalanced datasets. IEEE Trans. Softw. Eng. **24**(4), 278–301 (1998)
9. K. Lee, M. Rucker, W.T. Scherer, P.A. Beling, M.S. Gerber, H. Kang, Agent-based model construction using inverse reinforcement learning, in *2017 Winter Simulation Conference (WSC)* (2017), pp. 1264–1275
10. Y.J. Lin, P.W. Wu, C.H. Hsu, I.P. Tu, S.w. Liao, An evaluation of bitcoin address classification based on transaction history summarization, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2019), pp. 302–310
11. J. Lorenz, M.I. Silva, D. Aparício, J.T. Ascensão, P. Bizarro, Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity (2020). Preprint arXiv:2005.14635
12. G. Mariani, F. Scheidegger, R. Istrate, C. Bekas, C. Malossi, Bagan: Data augmentation with balancing GAN (2018). Preprint arXiv:1803.09655
13. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage, A fistful of bitcoins: Characterizing payments among men with no names, in *Proceedings of*

[3] https://github.com/onezerobinary/AML.

the 2013 Conference on Internet Measurement Conference (2013), pp. 127–140

14. D. Moore, T. Rid, Cryptopolitik and the darknet. Survival **58**(1), 7–38 (2016)
15. F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, E. Duchesnay, Scikit-learn: Machine learning in Python. J. Mach. Learn. Res. **12**, 2825–2830 (2011)
16. M. Ringnér, What is principal component analysis? Nat. Biotechnol. **26**(3), 303–304 (2008)
17. K. Toyoda, T. Ohtsuki, P.T. Mathiopoulos, Multi-class bitcoin-enabled service identification based on transaction history summarization, in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (2018), pp. 1153–1160
18. R. Van Wegberg, J.J. Oerlemans, O. van Deventer, Bitcoin money laundering: mixed results? J. Finan. Crime **25**(2), 419–435 (2018)
19. C. Wang, Q. Wu, S. Huang, A. Saied, Economical hyperparameter optimization with blended search strategy, in *ICLR'21 Conference Program Chairs* (2021)
20. C. Wang, Q. Wu, M. Weimer, E. Zhu, FLAML: A fast and lightweight AutoML library. Proceed. Mach. Learn. Syst. **3**, 434–447 (2021)
21. M. Weber, G. Domeniconi, J. Chen, D.K.I. Weidele, C. Bellei, T. Robinson, C.E. Leiserson, Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics (2019). Preprint arXiv:1908.02591
22. Q. Wu, C. Wang, S. Huang, Frugal optimization for cost-related hyperparameters, in *Proceedings of the AAAI Conference on Artificial Intelligence* (2021)

Multidimensional Blockchain: Construction and Security Analysis

Ilya Shilov and Danil Zakoldaev

1 Introduction

Cryptocurrencies and related technologies have appeared not a long time ago but have already gained a significant role in the sphere of information technologies. Among the most important features of blockchain technology, which emerged in 2008 with the invention of Bitcoin, was a consensus mechanism with resistance against 50% of adversarial users. This technology predefined the success of Bitcoin and its sustainable position [1].

On its basis a large number of related technologies had emerged. They applied various changes to the technology and its inner protocols. At the top of this development was the Ethereum project, which significantly transformed the principles of building decentralized systems. As mentioned by its authors, blockchain could be used not only for the construction of cryptocurrencies but for a wider range of spheres. The main advantage of Ethereum was a Turing-complete language, which had enriched blockchain with the possibility of programming.

In general, the following advantages of blockchain technology can be named:

1. Decentralization [6].
2. Reaching consensus in the presence of faults and adversarial actions.
3. The possibility of building decentralized applications.

These advantages attract business, technology companies, and financial corporations to blockchain and related systems. However, it is necessary to admit that blockchain is not deprived of disadvantages. Of those following have a special meaning:

I. Shilov (✉) · D. Zakoldaev
ITMO University, St. Petersburg, Russia
e-mail: ilia.shilov@itmo.ru; d.zakoldaev@itmo.ru

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_3

1. Unconstrained growth of blockchain size, which complicated its storage and leads to partial centralization due to high requirements for maintaining nodes.
2. Significant expenses for maintaining some consensus mechanisms.
3. Uncontrolled economical processes (applying to cryptocurrencies).
4. Presence of intermediaries in intersystem exchange.

A large part of research has been taken recently to overcome these problems. In particular, the IOHK company has proven the security (in probabilistic sense) of a system based on proof-of-stake consensus mechanism, which is by far less expensive than proof of work [2, 11, 17]. Other approaches to building less power-consuming consensus mechanisms have also been presented [5]. Uncontrolled economical processes are partially handled by the KYC and AML policies, which allow to partially deanonymize operations with cryptocurrencies and increase the trust to cryptocurrencies from business.

However, until the present day, the size of blockchain remains a complicated problem. Blockchain implies replication of the complete database of blocks on all nodes in the network. Moreover, it is necessary to have access to complete block history to verify the chain correctness. Although the attempts to solve this problem have been undertaken, the provided solutions either have not been presented or solve the problem partially. The problem of blockchain size is shown in Fig. 1.

The problem of intersystem exchange is of great importance. Now such operations require using intermediate parties or sidechains. In practice these approaches do not solve the problem but move it to another level of abstraction.

This chapter summarizes the main advances in the direction of solving these problems, which have been achieved by the author in recent years. The concept of multidimensional blockchain is shown, and its protocols and components are

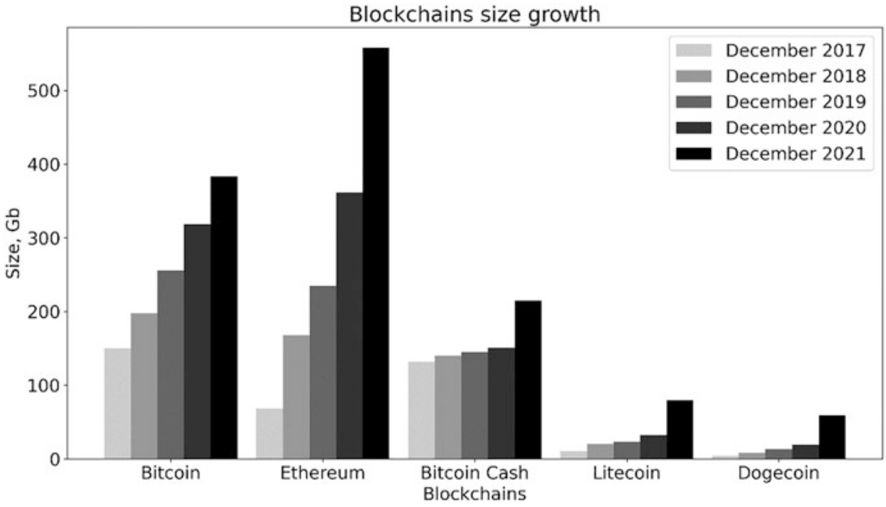


Fig. 1 Volume size growth for some famous systems based on the blockchain technology

described. Next, a brief overview of security analysis is given. On the basis of existing solutions, a novel search and verification protocol for blocks and transactions is presented, and its security is briefly examined. Finally, the experimental results and theoretical comparison for multidimensional blockchain and alternative systems are given.

2 Robust Distributed Ledgers

Before proceeding to the description and analysis of multidimensional blockchain, it is necessary to present several important terms used throughout the research. One of the most important applications of distributed systems is the *ledger*. In literature dedicated to research on consensus mechanisms, this term was created not a long time ago, and it is relatively rarely used in the sphere of cryptocurrencies.

In cryptocurrencies and database management systems, ledger is an ordered set of transactions. In practice ledgers are implicitly used in almost all database management systems. Moreover, a critical component of any automated banking system (ABS) is an ordered sequence of transactions, which also implies using a ledger. Finally, versioning systems, domain name systems, and many other distributed applications in some way use ordered sequence of transactions, which provides perspectives of using distributed ledgers. Distributed ledger is an evolution of ledger concept. It is a ledger maintained by two and more machines.

Robust distributed ledgers must comply with a set of requirements, of which the most important are persistence and liveness. These terms are based on the term of honest node – a node that acts in compliance with the protocol.

Persistence means that when an honest node declares some transaction as stable, all the other honest nodes also declare it as stable when queried. Persistence is presented as a predicate with parameter k. At first, persistence was created for distributed ledger based on blockchain. It meant that reaching depth of k blocks by transaction in a local copy of blockchain for honest node means that it occupies the same position in the same block in a local copy of blockchain for any other honest node. As robust distributed ledgers could be built on systems without the concept of block, later on this term has been generalized [13].

Liveness is a second feature of a robust distributed ledger, which preserves its robustness. It means guaranteed inclusion of honest user's transaction into ledger in an acceptable period (predefined number of time slots). In other words, liveness implies security against denial of including correct transactions into system by adversary's will. In application to blockchain, liveness implies guaranteed reaching of depth more than k blocks in a certain number of rounds by honest transaction.

For ledger controlled by one node, persistence and liveness are fulfilled by default. It is way more difficult to achieve these qualities for distributed ledgers functioning in an unreliable environment in the presence of adversaries operating against the protocol. Blockchain solves this exact problem.

3 Multidimensional Blockchain

Multidimensional blockchain is a system based on the concept of sidechains. Sidechain solutions have been created a while ago and are used mainly to transfer funds between independent cryptocurrencies. At first such operations were performed by observing the complete chain history in foreign blockchain. One of the first approaches to speed up this procedure was the use of nested hash chains (interlink) [15]. Instead of checking the complete chain history, only a chain of blocks with hash-sums less than $T/2^i$ is checked (T is a target hash-sum value for consensus mechanism). Thus, the complexity of verification is significantly reduced. In [16] the approach has been improved. The main advantage of the proposed solution was the possibility to verify a transaction with only one request to the target ledger. Moreover, several additional predicates that generalize the concept of verification have been proposed.

An approach to building proof-of-stake-based sidechains has been developed in [14]. That approach was compatible with the GHOST approach [22]. A formal definition of sidechain notion independent of consensus mechanism has also been presented.

The review of major modern pegged sidechain solutions has been undertaken in [3]. The solutions described have been based on cryptocurrencies and allowed temporary exchange of tokens. It implied freezing the tokens in one system and creating a corresponding number of tokens in a different chain. Also, almost all solutions under review represented applications and lacked security analysis.

In general, pegged sidechains imply following sequence of operations:

1. A user willing to use funds in sidechain sends them to a special address in his blockchain and proves the fact of sending to sidechain.
2. Exchange of tokens happens in sidechain – the account of the user is credited with a certain number of tokens.
3. If reverse exchange is necessary, it is performed analogously: the user sends tokens to a pre-defined address, where these tokens are frozen, and in an original blockchain, a transaction is created to return funds.

Multidimensional blockchain generalizes the concept of sidechains. It is a system consisting of a set of blockchains, where each blockchain, but the first one, follows the procedure of registration in one of the existing blockchains. Registration means storing information on genesis-block and, in some cases, information about some features of the new blockchain in some other blockchains.

The result system is in fact a tree of blocks. At the same time, many consensus algorithms permit temporary forks that lead to the existence of several syntactically correct chains in one blockchain – when correct and approved chain is only one of them. Taking this fact into account to avoid vagueness of term, the name "multidimensional blockchain" has been selected.

Two ways of building a multidimensional blockchain are possible: block mode and state mode. Figure 2 shows a general view of multidimensional blockchain,

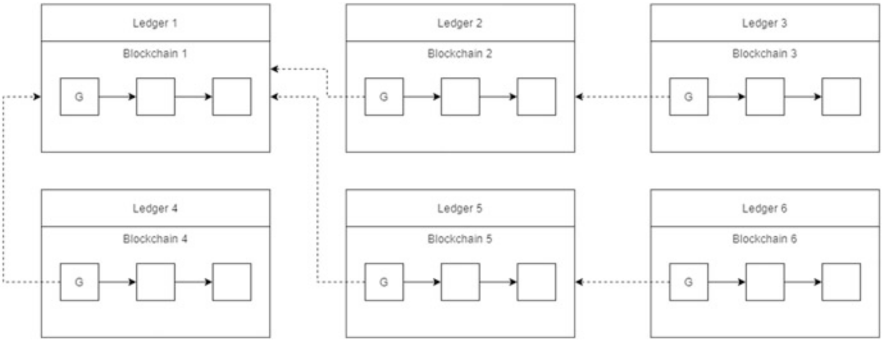


Fig. 2 Multidimensional blockchain

which unites several blockchains into one system. It is supposed that every blockchain implements robust distributed ledger – this assumption allows to disengage from a concrete operation mode. Therefore, it is not explicitly mentioned how exactly blockchain registration is performed: in block of special type or in internal data structure.

Block mode requires the creation of blocks of special type – for registration. State mode is based on the concept of state-transition machine developed in Ethereum white paper by G. Wood. It has been extended to represent a multidimensional blockchain. Consider the multidimensional blockchain mathematical model. As blockchains create new states at different rates, the following ratios assume that transactions were created within a fixed length of time, a slot. For the most correct statement of the mathematical model, the following relation can be taken:

$$\begin{gathered} T^{(k)} = \left(T^{(k,1)}, \cdots, T^{(k,j)}\right) \left| j = \left[\frac{\text{Time}\left(\sigma_t^{(k)} \to \sigma_{t+1}^{(k)}\right)}{\text{sl}} \right] \right. \\ \text{sl} \equiv \text{GCD}\ \left(\text{Time}\ \left(\sigma_t \to \sigma_{t+1}\right)\right), T^{(k,j)} = \left(T_0^{(k,j)}, \cdots, T_n^{(k,j)}\right) \end{gathered} \tag{1}$$

where $T^{(k,j)}$ is a transaction tuple in ledger k during slot j, sl is a time slot, GCD is a greater common divider function, Time is a function returning state transition duration, and σ is a state.

In other words, a slot is the largest period of time into which the time intervals necessary for the transition between states in all blockchains are completely divided. As a result, each transition between states in each blockchain occurs once in a fixed (integer) number of slots:

$$\Pi'\left(\sigma^{(k)}, T^{(k,j)}\right) = \begin{cases} \sigma^{(k)} \text{ if } T^{(k,j)} = \varnothing \\ \Omega\left(\Upsilon\left(\ldots\Upsilon\left(\Upsilon\left(\sigma^{(k)}, \mathrm{T}_0^{(k,j)}\right), \ldots\right) T_n^{(k,j)}\right)\right) \text{ otherwise} \end{cases} \tag{2}$$

where $\Pi^{'}$ is a modified block-level state transition function, Υ is a state transition function, and Ω is a finalizing function responsible for consensus mechanism. In general, a multidimensional blockchain can be represented as follows:

$$\Sigma_{i+1} \equiv \Phi\left(\Sigma_i, T\right) \mid \Sigma_i \equiv \left\{\sigma^{(1)}, \ldots, \sigma^{(N)}\right\} \wedge \Phi\left(\Sigma_i, T\right) \equiv \Psi\left(\mathrm{P}\left(\Sigma_i, T\right), T\right) \tag{3}$$

$$\mathrm{P}\left(\Sigma_i, T\right) = \mathrm{E}\left(\mathrm{E}\left(\ldots \mathrm{E}\left(\Sigma_i, T, 1\right), \ldots\right) T, N\right) \mid \mathrm{E}\left(\Sigma_i, T, k\right) = \mathrm{E}'\left(\Pi'^{\left(\sigma^{(k)}, T\right)}\right), \tag{4}$$

where Ψ creates new blockchains, P is a state transition function, E is a state transition function for the k-th blockchain in its composition, and $\mathrm{E}^{'}$ is an auxiliary function that returns a multidimensional blockchain for a one-dimensional blockchain and is used to avoid using the universal quantifier in mathematical notation. Finally, let us define the relationship between the state transition functions of ledgers:

$$\Pi\left(\sigma^{(k)}, T^{(k)}\right) = \Pi'\left(\Pi'\left(\ldots \Pi'\left(\sigma^{(k)}, T^{(k,1)}\right), \ldots\right), T^{(k,j)}\right)\right) \tag{5}$$

A key feature of a multidimensional blockchain is addressing, which directly affects the order in which applications are built. Within the framework of a multidimensional blockchain, user accounts, transactions, blocks, blockchains, and nodes supporting the system are subject to addressing. Addressing is performed in hierarchical mode, and a special notation has been developed to distinguish the addressed entities. A deep representation of the addressing has been shown in [18].

It is necessary to outline the fact that every blockchain is still a one-dimensional list that can operate separately from the system and differs from general implementations only, thanks to typing or existence of registration storage – depending on the operation model. At least two ways of addressing exist:

- Absolute – in multidimensional blockchain.
- Relative – in the current blockchain.

Besides, if in any subsystem interaction with a large number of other subsystems is not intended, using full address for every block can become excessive – especially at late functioning stages and in blockchains that are situated deep in the nested structure. In this case, it is possible to use aliases that are known to all participants of current subnet.

In block mode, addressing of child blockchain is possible using a number or a hash sum of block that performs registration of child blockchain. Number means height of block in parent blockchain where the current blockchain is registered. Both approaches are identical, but using hash sum allows to avoid reading all the blockchain and works faster in general. Also, if several blockchains are registered in one block, it is necessary to specify the blockchain registration number inside the block. Special designation is to be used in this case.

In state model, every blockchain is registered by placing genesis-block or its hash sum into another blockchain. Child blockchain can be referenced by its genesis-block hash sum. The uniqueness of hash sums is provided by the hashing algorithm in use – and it is chosen while designing a concrete implementation. Cryptographic hash algorithms guarantee the existence of collisions with negligible probability, which leads to practically guaranteed uniqueness of genesis-block hash sum throughout the multidimensional blockchain provided that the genesis-blocks are unique. Theoretical addressing can be built using non-unique hash sums, but this might lead to double-spent vulnerability. In case double-spent attacks are not actual, using non-unique hash sums is permitted.

The main feature of a multidimensional blockchain is the presence of external transactions. An external transaction is an ordered sequence of logically related write-and-read operations in two or more ledgers. The ledger in which the external transaction starts is called the initiator, and the ledgers that accept the transaction are called recipients or acceptors. An external transaction, respectively, consists of two phases – initiation and acceptance (reception). It is worth noting that any external transaction always has one initiator, but there can be several recipients.

Consider the algorithm for conducting an external transaction in a multidimensional blockchain (Fig. 3). For the correct acceptance of a transaction in the acceptor ledger, it must be present in the initiating ledger, and the transaction must not have been accepted before.

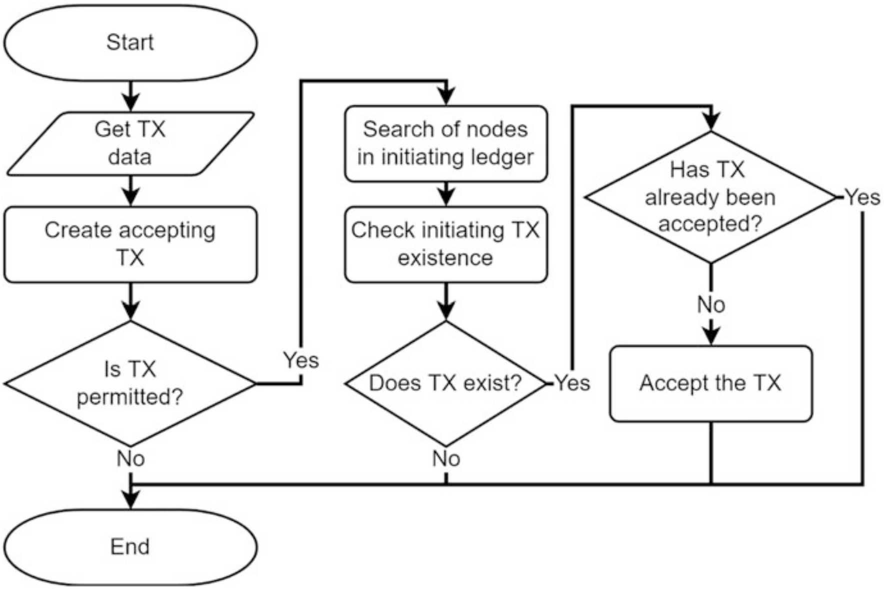


Fig. 3 Algorithm of accepting phase for external transaction

To sum up, multidimensional blockchain is a system based on the concept of one-dimensional blockchain and is meant to perform secure intersystem exchange and scaling of the systems based on distributed ledgers. The security is provided by the underlying data structure and a set of protocols for search and verification of external transactions.

4 Multidimensional Blockchain Security Analysis

The security analysis of multidimensional blockchain has been divided into several directions. First, it is necessary to show how the security of separate robust distributed ledgers is affected in case of scaling with multidimensional blockchain. This analysis is important as some security parameters might change, thanks to the change in relation between honest and adversarial nodes. Second, it is required to examine security of intersystem exchange organized with multidimensional blockchain. Finally, an analysis of scaling security must be performed to show that multidimensional blockchain implements robust distributed ledger.

4.1 Security Analysis of Underlying Robust Distributed Ledgers

The first security assessment of blockchain technology (e.g., internal consensus mechanism – proof of work) was presented in the first work on the first widespread cryptocurrency by Satoshi Nakamoto. When scaling using a multidimensional blockchain, the nodes that support the system are split into groups. As a result, the relation between the number of honest and adversarial nodes changes. Consequently, the parameters of the system change, which leads to a change in the probability of an attack. For a multidimensional blockchain, this probability takes the following form (modified version of probability calculated by Satoshi Nakamoto):

$$P_a = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{\frac{p}{N}}\right)^{(z-k)}\right), \tag{6}$$

where p and q are the probabilities of an adversarial and honest creating a block, respectively; N is the number of blockchains in a multidimensional blockchain; and z is the block depth for which the probability is calculated. An example of the probability of an attack on the last six blocks from the end of the chain is shown in Fig. 4.

The GHOST (Greedy Heaviest-Observed Subtree) approach has been developed by Zohar and Sompolinsky during their security assessment of Bitcoin and its

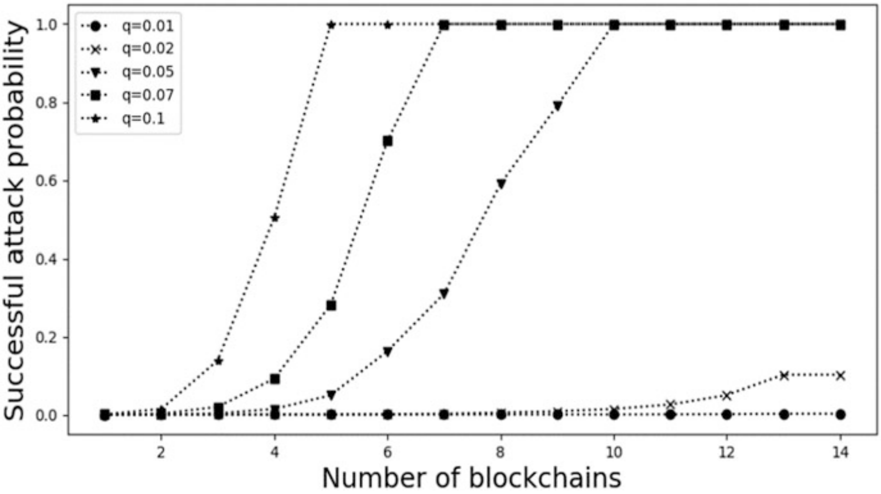


Fig. 4 Probability of a successful attack when the number of nodes is insufficient

underlying protocols [22]. It has been shown that standard chain selection rule is vulnerable to a potential attack of 25% of adversarial power. The novel approach implies placing in each block not only a hash-sum of a previous block but hash-sums of last blocks in recent forks. As a result, the discovered attack on Bitcoin and similar systems becomes impossible. The general safety condition is as follows:

$$\beta\left(\lambda_{\text{rep}}\right) \geq \frac{q}{1-q}\lambda_{\text{rep}} = \frac{q}{p}\lambda_{\text{rep}}, \tag{7}$$

where β is the block inclusion rate, λ_{rep} is the observed block creation rate, q and p are the probabilities that the next block is created by the attacker or honest node, respectively. Dividing miners into groups when creating a multidimensional blockchain (and when creating blockchains within a multidimensional blockchain) entails a change in the ratio of p and q, i.e., the probabilities of creating the next block by honest and attacking nodes. This leads to strengthening of the security requirement.

A more complete analysis of the proof of work has been presented by the IOHK company. The main requirement for the model is to comply with the requirements of honest majority:

$$t \leq (1-\delta)(n-t), \quad \delta \geq 2f + 2\epsilon, \tag{8}$$

where t is the number of compromised nodes, n is the total number of nodes, f is the expected number of new blocks created in each round, and ϵ is a negligible number. When the blockchain is split into independent blockchains inside multidimensional blockchain, the number of honest nodes decreases, which leads to a decrease in the parameter *f*. Consequently, the lower bound of the parameter δ decreases, which entails the strengthening of the requirement for an honest majority.

The security of a proof-of-stake system does not depend on the number of nodes maintaining it and is determined by the number of accounts in the system and the ratio between the shares of honest and attacker accounts. Therefore, the theorems introduced in the articles about Ouroboros remain correct for a multidimensional blockchain under the only condition – the creation of a genesis block with a fair majority when registering a new blockchain.

A more deep and thorough analysis has been presented in [19].

4.2 Intersystem Exchange Security Analysis

To prove the security of a multidimensional blockchain, it is required to show that it does not break the security of internal robust distributed ledgers with the novel functionality of external transactions. In other words, it is necessary to show that the intersystem exchange is secure. To achieve this goal, a generalized universal composition framework (GUC-framework) is used. It involves representing the system in the form of a set of interacting interactive Turing machines and proving either of the following:

1. For any adversarial node attacking the target system (ideal functionality), there exists a simulator attaching the constructed protocol such that it is impossible for an environment (external observer) to distinguish the executions (in probabilistic sense).
2. There exists a sequence of equivalent hybrid models from the target system model to the constructed protocol model. A hybrid model incorporates parts of both target and constructed systems.
3. The probability of bad events that might break some security requirements is negligible in probabilistic sense (in this case, the GUC model is used to perform formalization).

A deep description of the GUC framework has been presented in [7, 8] and some other papers in which the security analysis has been performed with the help of it [9, 10]. It is worth mentioning that the models of robust distributed ledgers have been presented in the literature before [2, 4, 12]. However, these functionalities have not implemented external transactions. Thus, a novel robust distributed ledger model has been built to prove the security of multidimensional blockchain. It supports external transaction functionality and is constructed as close to the pre-invented models as possible. Also, a model for a protocol implementing robust distributed ledger has been created. In addition, an auxiliary ideal functionality for searching and verifying external transactions was proposed.

Both models – of ideal functionality implementing robust distributed ledger and corresponding protocol – are presented in Fig. 5. These models include the following parties: G_{CLOCK} is a timing ideal functionality, G_{VERIFY} is an ideal func-

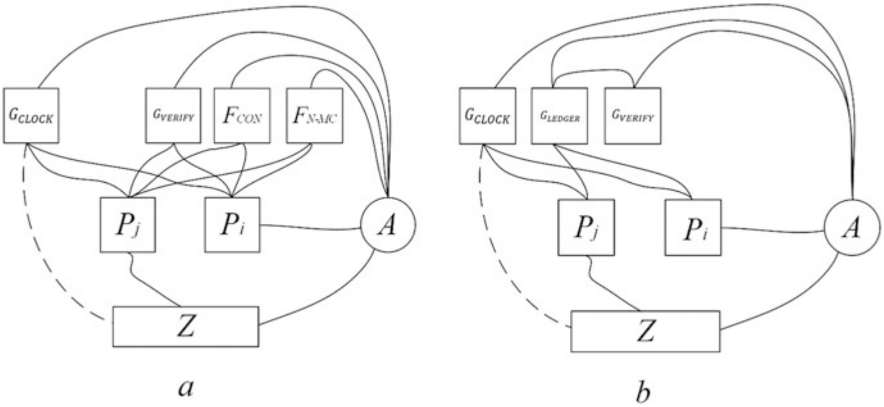


Fig. 5 GUC-model of protocol implementing robust distributed ledger (**a**) and GUC-model of robust distributed ledger (**b**)

tionality used for search and verification, F_{CON} is consensus mechanism, $F_{N-\mathrm{MC}}$ is multicast medium, G_{LEDGER} is robust distributed ledger (which implements external transactions), A is adversary, Z is environment, and P_i are the parties running the model.

With these models, the following propositions have been proven:

1. The robust distributed ledger model is compatible with previously proposed models.
2. The properties of persistence and liveness are not violated when using the ideal search and verification functionality for blocks and transactions with a probability proportional to the probability of a fork at depth k.

The first proposition has been proven by comparison of the execution models. It is sufficient to show that these have no differences but external transactions [21]. The proof leads to the proof of the second proposition. The second proof is based on the examination of possible "bad" events that might break the properties of persistence and liveness (the proof is shown as it has not been presented before):

- *BAD1* – breaking liveness of the initiating ledger. This event is impossible, thanks to the way the external transactions are performed (the initiating phase is equal to ordinary transaction).
- *BAD2* – breaking liveness of accepting ledger. This event is impossible because ideal functionality provides guaranteed verification in case the verification period exceeds the provided time window. For this to happen, the following relation must hold:

$$\text{window} \times t_{\mathrm{sl}} - 1 \geq \max\{d\} \times 2 \times \max\{t_v\}\,, \qquad (9)$$

where window is a window size in slots, t_{sl} is a slot duration, d is the maximum ledger depth, and t_v is the time of interaction with ledger during search or verification.

- *BAD3* – breaking persistence of the initiating ledger. This event is impossible, thanks to the way the external transactions are performed (the initiating phase is equal to ordinary transaction).
- *BAD4* – breaking persistence of the accepting ledger. As the response on verification of external transactions is delayed, the only way to break persistence is to apply transaction to the ledger and to revert it in the initiating ledger. All the ledgers in multidimensional blockchain are robust by assumption. Thus this situation is possible only when the transaction is reverted before going deep enough in the chain of blocks. Let $p^{(k)}$ be the probability of fork at depth k. Then the probability of acknowledgement is as follows:

$$p = p^{(k)} \times \frac{\sum \theta_i^H + \gamma \sum \theta_i^A}{|H| + |\, A \,|} \tag{10}$$

In the worst case, the nodes are split into two equally sized groups such that in one of them, there are all the adversarial nodes and sufficient number of honest nodes. Then the adversary has a maximum chance of reverting transaction:

$$\begin{cases} \sum \theta_i^A = |\, A \,| \\ \sum \theta_i^H = 0,5 \times (|H| + |A|) - |A| = 0,5\,(|H| - |A|) \end{cases} \Rightarrow p = p^{(k)} \times 0,5 \tag{11}$$

Finally, for a protocol that is executed by nodes supporting a multidimensional blockchain, the GUC-model has also been proposed:

A proposition has been proven that this protocol GUC-implements the ideal functionality of a multidimensional blockchain. To prove this, it is enough to show that the execution of this protocol is equivalent to the execution of the multidimensional blockchain GUC-model, because in this case, the universal composition theorem will be applicable. The proof is based on hybrid models, when each next model differs from the previous one but remains equivalent to it (the proof is shown as it has not been presented before):

- HYB0 is a multidimensional blockchain model. All nodes use queries to the multidimensional blockchain to work. In fact they act like "dummy" parties that only pass queries in an appropriate format to an ideal functionality.
- HYB1 is a model in which nodes independently handle addressing actions, i.e., determine source and destination ledgers for each external transaction. Instead of one external transaction, they redirect two internal transactions (outgoing and incoming) to the multidimensional blockchain. HYB1 is equivalent to HYB0, because the way the model uses multidimensional blockchain does not change: external transactions are simply divided in advance.

- HYB2 is a model in which nodes perform notifications on all external transactions: when a new transaction is created, a notification is sent to the nodes that maintain the target ledger. Then they independently send a request to the multidimensional blockchain. The difference from HYB1 is only in the origin of the second (incoming) transaction, because the transmission of the notification takes negligible time in the scale of the slot time.
- HYB3 is a model in which nodes independently verify an external transaction and send a request to add an incoming transaction only if it is correct. For this, the ideal search and verification functionality is used, which is guaranteed to carry out the verification correctly. The same functionality is used inside multidimensional blockchain ideal functionality. Because no changes have been made to the functionality of the multidimensional blockchain, this model is equivalent to HYB2.
- HYB4 is a model in which nodes independently carry out verification of incoming external transactions using a search and verification protocol, which must GUC-implement an ideal search and verification protocol. According to the universal composition theorem, this model is equivalent to HYB3 with a probability determined by the probability of successful verification.
- HYB5 is a model in which the multidimensional blockchain is replaced by many one-dimensional blockchains. Because verification is guaranteed (subject to the constraints of the GUC-implementation), this model is equivalent to HYB4.

It can be seen that HYB5 is the same model as that given in Fig. 6. In other words, this model is actually a simulated protocol that implements a multidimensional blockchain (MBC-Protocol). Thus the MBC-Protocol GUC-implements ideal multidimensional blockchain functionality and can be used in models instead of this functionality and vice versa.

4.3 Scaling Security Analysis

Yet multidimensional blockchain has been invented to perform intersystem exchange; it also solves the problem of scaling robust distributed ledgers. To prove the security of scaling, it is sufficient to show that multidimensional blockchain GUC-implements robust distributed ledger. In this case a one-dimensional blockchain GUC-implementing robust distributed ledger can be replaced by multidimensional blockchain.

To build such a proof, a simulating approach was used: it has been proven that for any node attacking a multidimensional blockchain, there exists a simulator attacking the ideal functionality of a robust distributed ledger that, from the side of the environment, the two executions are identical. A schematic representation of the simulation model is shown in Fig. 7.

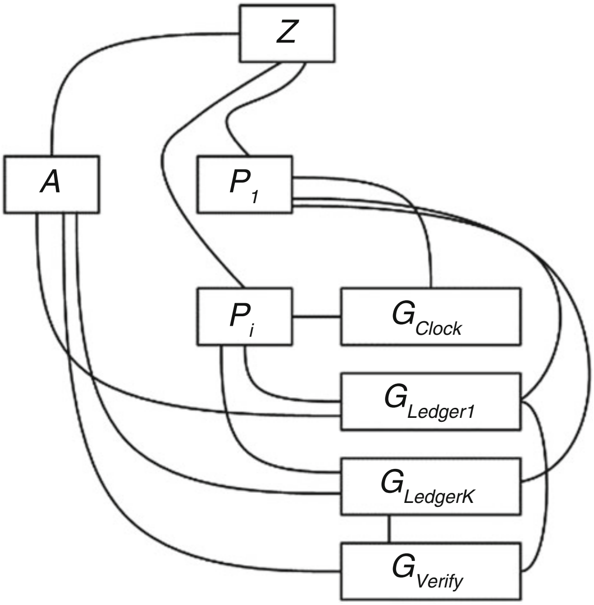


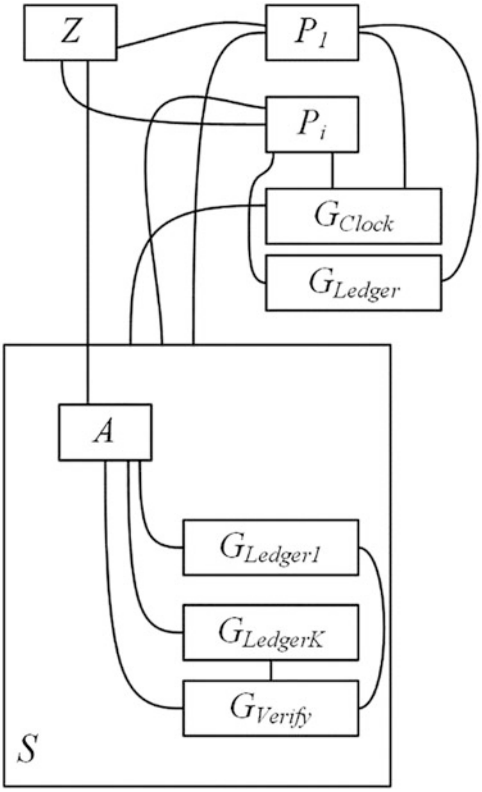
Fig. 6 GUC-model of a protocol implementing multidimensional blockchain (MBC-Protocol)

5 Search and Verification Protocol

In [20] several approaches to building search and verification protocol for blocks and transactions have been presented. The following conclusions were obtained:

1. A centralized search and verification protocol is equivalent to ideal functionality, provided that the node supporting the protocol is honest.
2. The search and verification protocol for blocks and transactions built on the basis of a fully connected network interaction graph GUC-implements an ideal search and verification protocol for blocks and transactions with the probability specified in Relation (12).
3. The search and verification protocol for blocks and transactions, built on the basis of a fully connected graph of network interaction with the parent blockchain, GUC-implements an ideal search and verification protocol for blocks and transactions with the probability indicated in Relation (12).
4. The 1-to-1 connection approach is not secure and should not be used when building a search and verification protocol for blocks and transactions.
5. The approach with connecting subsets of neighboring ledgers is not secure and should not be used when building a search and verification protocol for blocks and transactions.

Fig. 7 GUC-model of a system with a simulator



$$P = \begin{cases} \sum_{i=0}^{\left[\frac{k}{2}\right]-1} C_k^i \times q^i \times p^{k-i}, \text{if } z = \left[\frac{k}{2}\right] - 1 \leq N_A \\ 1, \text{if } \left[\frac{k}{2}\right] - 1 > N_A \end{cases}, \tag{12}$$

where k is the number of polled nodes, p is the proportion of honest nodes, q is the proportion of attacking nodes, C is the number of combinations, and N_A is the number of attackers.

A robust search and verification protocol for blocks and transactions has been invented. This protocol makes it possible to guarantee the search for nodes of the target registry and, under certain conditions, to carry out verification faster than using a sidechain-based solution. The following version of the protocol is proposed:

1. Each blockchain node keeps track of the last $l + 2k$ blocks from each neighboring blockchain. k blocks are used to provide the common prefix property. l blocks correspond to the chain quality.
2. They are asked for the headers of $l + 2k$ blocks in the next blockchain and the addresses of the nodes that created them (identifiers and a network entry point for

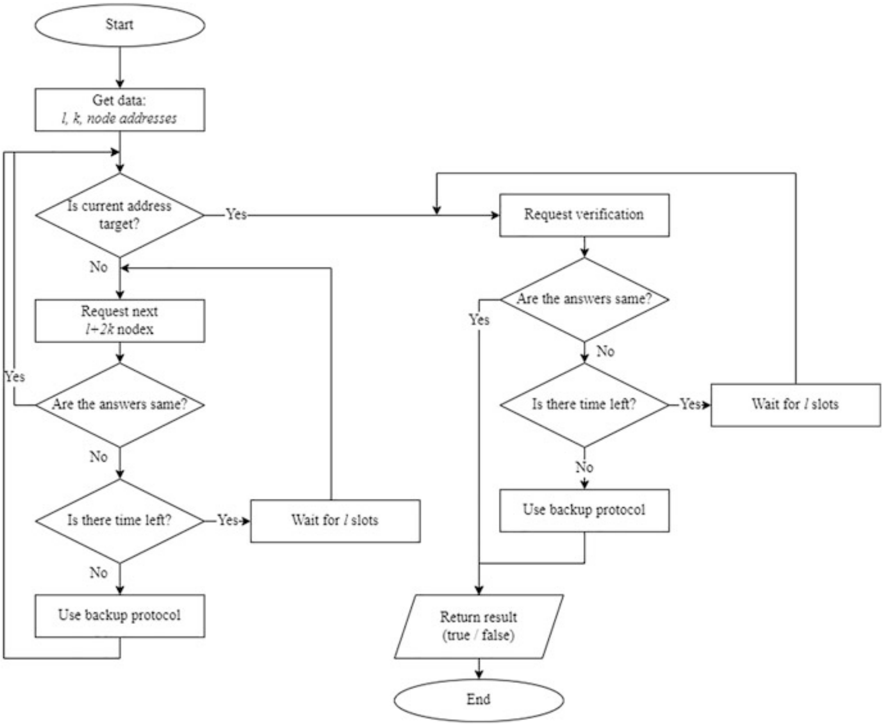


Fig. 8 Robust search and verification protocol for blocks and transactions

searching are allowed). The last k blocks are used to comply with the common prefix property, the next l blocks are used to enforce the purity property of the chain, and the last k blocks are needed for verification. Because there is at least one honest node among the nodes (by the CQP, because the length is greater than l), such a chain is guaranteed to exist. For the obtained blocks, the correctness of their construction is checked.

3. If the ledger is targeted, then go to the next step. Otherwise, select l nodes in the middle of the resulting chain, and go to step 1.
4. If the combined search and verification time exceeds the maximum allowable time in terms of liveness, perform verification using the backup functionality.
5. To verify the l found nodes (which created l blocks deeper than the last k) in the block chain, a chain of $l + 2k$ blocks is requested.
6. If the $l + k$ first blocks are the same among all the received results, perform verification by requesting the block containing the outgoing transaction and the chain of headers from this block to the first among $l + k$ received earlier. Otherwise, skip l slots and go to step 1.

The algorithm is shown in Fig. 8.

Using the universal composition framework, the following propositions have been proven:

1. The robust search and verification protocol makes it possible to correctly verify an external transaction with a probability close to 1, with the right choice of the set of polled nodes.
2. The robust search and verification protocol based on the chain quality property implements the ideal search and verification functionality with the probability of maintaining the chain quality by the blockchains included in the multidimensional blockchain.

By the definition of a multidimensional blockchain, all ledgers within it are stable. A ledger is stable if it meets the Chain Growth (CGP), Common Prefix (CPP), and Chain Purity (CQP) requirements. Consider possible attacks on the protocol by an attacker.

Event 1: The attacker forms a completely fabricated chain of length $l + 2k$. This event can only occur if the purity property of the chain is violated. Therefore, the probability of this event in the worst case is as follows:

1. $p_1 = 1 - (1 - e^{-\Omega(\kappa)}) = e^{-\Omega(\kappa)}$ for proof of work (this upper bound is less than other from analogous works, e.g., [12]).
2. $p_1 = 1 - \left(1 - e^{-\Omega\left(\sqrt{l+k}\right)+\ln R}\right) = e^{-\Omega\left(\sqrt{l+k}\right)+\ln R}$ for proof-of-stake (by Theorem 4.13 of [17]).

Event 2: All polled nodes are attackers. This event can only occur if the chain quality property of the chain is violated. Therefore, the probability of this event in the worst case is as follows:

1. $p_2 = 1 - (1 - e^{-\Omega(\kappa)}) = e^{-\Omega(\kappa)}$ for proof of work (this upper bound is less than other from analogous works, e.g., [12]).
2. $p_2 = 1-\left(1 - e^{-\Omega\left(\sqrt{l+k}\right)+\ln R}\right) = e^{-\Omega\left(\sqrt{l+k}\right)+\ln R}$ or proof of stake (by Theorem 4.13 of [17]).

Event 3: The attacker generates an alternative chain of blocks when requesting information from block N to block *N-l-2k*. This event is determined by the probability of finding the first preimage for the hash sum used in the blockchain. In the worst case, this probability is equal to $p_3 = \left(\frac{1}{2^{\kappa}}\right)^{l+2k}$.

Event 4: Two honest nodes provide different responses to the query. This situation can only occur if the common prefix property is violated. Because nodes that created blocks at depth k are used for interaction, the probability of this event is as follows:

1. $p_4 = 1 - \left(1 - e^{-\Omega^{\kappa}}\right) = e^{-\Omega(\kappa)}$ for proof of work (this upper bound is less than other from analogous works, e.g., [12]).
2. $p_4 = 1 - (1 - e^{-\Omega(\kappa) + \ln R}) = e^{-\Omega(\kappa) + \ln R}$ for proof of stake.

Event 5: The attacker does not provide information when requested. This event causes the fallback protocol to be used and therefore does not compromise system security. In this case, in the worst case, the probability of an event depends on the probability of the presence of at least one attacker (in the worst case, *0.5l*) and is therefore not negligible.

Therefore, the probability of violating the information security and robustness properties of a distributed ledger for proof of work and proof of stake, respectively, is as follows:

$$P_{\mathrm{POW}} = p_1 + p_2 + p_3 + p_4 = 3 \times \mathrm{e}^{-\Omega(\kappa)} + \left(\frac{1}{2^{\kappa}}\right)^{l+2k} \approx \varepsilon \tag{13}$$

$$P_{\mathrm{POS}} = p_1 + p_2 + p_3 + p_4 = 2 \times \mathrm{e}^{-\Omega\left(\sqrt{l+k}\right)+\ln R} + \left(\frac{1}{2^{\kappa}}\right)^{l+2k} + e^{-\Omega(\kappa)+\ln R} \approx \varepsilon \tag{14}$$

The second proposition is proven with the help of hybrid models:

- HYB0 is the original model; external interactions are carried out using the ideal functionality to validate external transactions.
- HYB1 is a model in which the nodes themselves provide work with the search for ledgers for interaction. However, all ledgers still notify the ideal functionality about external transactions. As a result, each node using the search protocol can be guaranteed to discover a subset of the initiating ledger nodes, i.e., the search is performed independently, while verification is still performed using ideal functionality. Since the search is carried out correctly with a probability close to 1, for an external observer, this model is equivalent to HYB0.
- HYB2 – separation of transaction validation logic. Instead of ideal functionality, a wrapper is used that executes a set of ideal functionalities within itself, each of which is passed requests related to only one ledger. External interfaces do not change, so the model is equivalent to HYB1.
- HYB3 – wrapper elimination. Ledgers interact independently with ideal functionalities. Information about which ideal functionality to request verification from is requested from the nodes found through the search protocol. The search and verification protocol searches with the probability of respecting the chain quality and common prefix properties. According to the previous proposition, this probability is close to 1.
- HYB4 – requesting information directly from nodes. Similarly to HYB3, information is requested from the nodes; however, it is information about the correctness of the transaction that is requested. The probability of correct verification remains the same, because honest nodes follow the protocol and correctly verify the transaction. This model is equivalent to a search and verification protocol for blocks and transactions.

6 Theoretical and Experimental Analysis

Multidimensional blockchain has several advantages over conventional systems. This section covers them. Consider saving memory by a separate node of a computer network when replacing a one-dimensional blockchain with a multidimensional analogue. Let the source ledger be divided into N_L ledgers. If the transaction generation period (frequency) or the block size decreases, then the average value of the amount of information stored by the nodes at any given time is as follows:

$$\overline{\mathrm{LV}} = \frac{\sum_i \mathrm{LV}^{(i)}}{N_L} = \frac{LV \times \sum_i p_i}{N_L} = \frac{LV}{{N_L}'} \tag{15}$$

where N_L is the number of registries, and p_i is the number of accounts transferred to the new blockchain. Figure 9 shows comparison of the volume size growth for the different numbers of ledgers inside the multidimensional blockchain.

Another important feature of any ledger is the number of transactions per second (TPS). Figure 10 shows an estimate of the TPS. In each unit of time, the number of blockchains increases by 1. Graphs 1 and 2 reflect the increase in the number of transactions per unit of time in the system as a whole with a constant increase in the number of transactions and without growth, respectively. Graphs 3 and 4 reflect the reduction in the load on each blockchain separately under the same conditions. A more comprehensive analysis has been presented in [18].

In order to verify the applicability of multidimensional blockchain, an experimental analysis has been conducted. For this, a prototype that implements a multidimensional blockchain was applied. It implemented a simple token-based system with accounts associated with key pairs and balances.

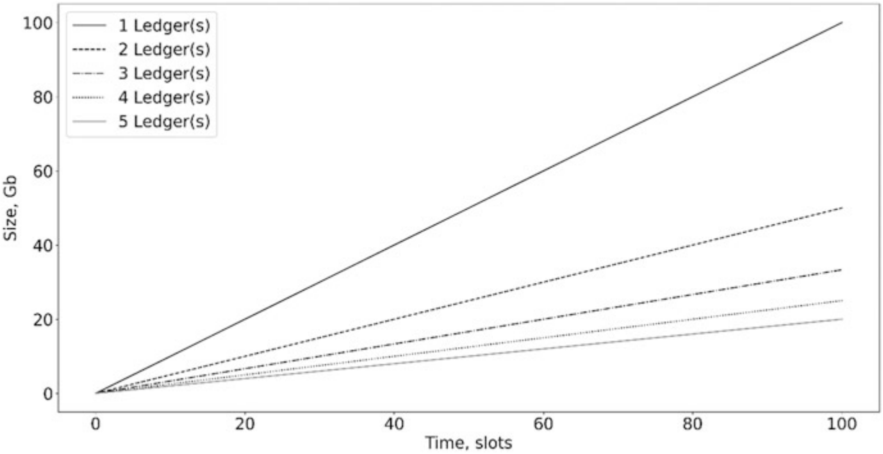


Fig. 9 Volume of one node for the different numbers of blockchains

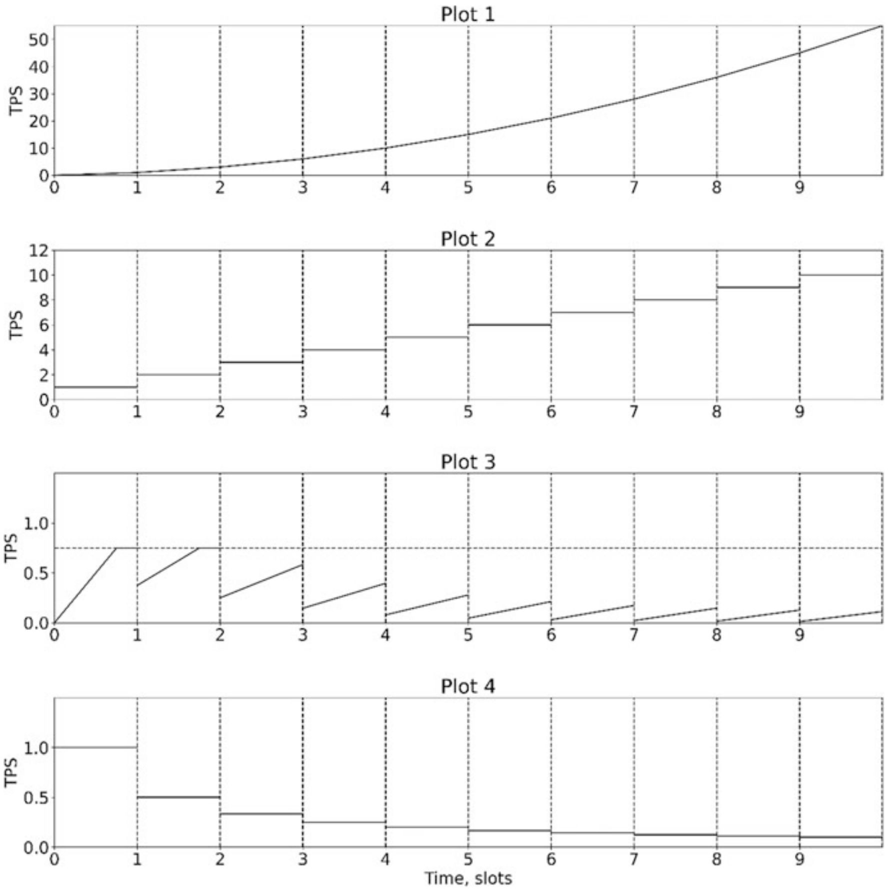


Fig. 10 TPS in multidimensional blockchain

A series of experiments were conducted to test the properties of a multidimensional blockchain. As part of the first experiment, five independent robust ledgers were used, each of which was executed by five nodes in different parts of the world. It is necessary to admit that the system was based on simple centralized consensus mechanism (beacon service) in order to decrease the influence of consensus scheme peculiarities on the analysis. Also search and verification errors have been modeled by a probabilistic approach: a probability of unsuccessful search and verification has been introduced. The sequence of transactions has been generated programmatically, and for each ledger, a period of intensive transaction generation has been introduced.

The purpose of the first experiment was to identify the numerical characteristics of the system operation. All external transactions have been accepted. The average results for all ledgers are presented below (Table 1).

Table 1 Experimental results for external transaction delay (intersystem exchange)

Experiment	Delay	Delay of internal transactions, sec	Delay of external transactions verification, sec	Delay of external transactions applying, sec
No adversarial actions	Maximum	20.171	140.608	276.836
	Minimum	0.001	6.325	6.997
	Average	6.923	59.904	71.632
Adversarial actions	Maximum	20.009	260.179	339.509
	Minimum	0.001	6.303	6.82
	Average	5.042	65.716	80.989

Table 2 Experimental results for external transaction delay given the transaction rate growth (scaling)

Number of ledgers	Average transaction delay, sec	Maximum transaction delay, sec	Average storage load (number of TX stored)	TPS
1	4.97	10.15	313	0.21667
2	36.08	86.94	425.5	0.42083
3	15.57	80.32	350	0.52847
5	11.97	80.25	331	0.92847

Table 3 Experimental results for external transaction delay given the constant transaction rate (scaling)

Number of ledgers	Average transaction delay, sec	Maximum transaction delay, sec	Average storage load (number of transactions stored)	TPS
1	4.31	10.09	310	0.21806
2	36.14	80.38	229	0.21111
3	16.57	79.22	116.67	0.18194
5	12.02	80.09	67.4	0.1875

The second experiment was aimed at analyzing similar parameters under conditions of a targeted attack on the protocol by 10% of attackers (without using a backup protocol). All the other characteristics were left untouched. The results are presented in Table 2.

For scaling, an experimental test was also carried out using four models consisting of one, two, three, and five blockchains, respectively (the total number of nodes is unchanged). At the same time, a situation was considered in which the load on each independent blockchain is higher (the flow of transactions increases in proportion to the increase in the number of ledgers) or remains unchanged (Table 3).

Based on the experimental results, the following conclusions can be made:

1. Multidimensional blockchain allows to perform secure intersystem exchange with acceptable (under certain circumstances) average transaction delay.
2. Multidimensional blockchain allows to increase the system throughput.
3. Multidimensional blockchain allows to decrease requirements for nodes.
4. The split into multidimensional blockchain containing two ledgers leads to the opposite effect: the size of blockchain volume increases for all nodes thanks to the two-phase structure of external transactions.

7 Conclusion

This chapter covers the recent advances in the sphere of constructing multidimensional blockchain. The technology is briefly described, and its peculiarities are highlighted. Several statements on multidimensional blockchain security have been proven. Some proofs have been presented for the first time. Finally, experimental analysis of multidimensional blockchain functioning has been presented for the first time.

In general, multidimensional blockchain allows solving the problem of scaling robust distributed ledgers and the problem of secure exchange between independent robust distributed ledgers. The research and its results described in this chapter are of interest to developers of decentralized and distributed technologies and applications, as well as researchers involved in the problem of secure intersystem interaction and questions of building distributed technologies.

As prospects for further development, we can point out the improvement of the proposed search and verification protocol for blocks and transactions in order to increase the likelihood of its successful operation in the face of attacks from malicious network nodes. In addition, it is of interest to introduce zero-knowledge cryptographic methods into the process of conducting external transactions to ensure the confidentiality of transactional information. Finally, it is possible to search for new areas for applying the proposed methods and algorithms and adapt them accordingly.

References

1. A. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Crypto-Currencies* (O'Reilly Media, Inc., Sebastopol, 2014)
2. C. Badertscher, P. Gaži, A. Kiayias, A. Russell, V. Zikas, Ouroboros genesis: composable proof-of-stake blockchains with dynamic availability, in *ACM Conference on Computer and Communications Security – ACM CCS 2018* (2018), pp. 913–930
3. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timon, P. Wuille, Enabling blockchain innovations with pegged sidechains. https://blockstream.com/sidechains.pdf. Retrieved March, 2022

4. C. Badertscher, U. Maurer, D. Tschudi, V. Zikas, Bitcoin as a transaction ledger: a composable treatment, in *Advances in Cryptology – CRYPTO 2017, LNCS*, vol. 10401, (Springer, Cham, 2017), pp. 324–356
5. I. Bentov, A. Gabizon, A. Mizrahi, Cryptocurrencies without proof of work, in *Financial Cryptography and Data Security, FC 2016, LNCS*, vol. 9604, (Springer, Berlin, Heidelberg, 2016), pp. 142–157
6. C. Cachin, R. Guerraoui, L. Rodrigues, *Introduction to Reliable and Secure Distributed Programming* (Springer-Verlag, Berlin, Heidelberg, 2011)
7. R. Canetti, Universally composable security: a new paradigm for cryptographic protocols, in *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, Newport Beach (2001), pp. 136–145
8. R. Canetti, Y. Dodis, R. Pass, S. Walfish, Universally composable security with global setup, in *Theory of Cryptography, TCC 2007, LNCS*, vol. 4392, (Springer, Berlin, Heidelberg, 2007), pp. 61–85
9. R. Canetti, D. Shahaf, M. Vald, Universally composable authentication and key-exchange with global PKI, in *Public-Key Cryptography – PKC 2016, PKC 2016, LNCS*, vol. 9615, (Springer, Berlin, Heidelberg, 2016), pp. 265–296
10. B. David, R. Dowsley, M. Larangeira, ROYALE: a framework for universally composable card games with financial rewards and penalties enforcement, in *Financial Cryptography and Data Security, FC 2019, LNCS*, vol. 11598, (Springer, Cham, 2019), pp. 282–300
11. B. David, P. Gaži, A. Kiayias, A. Russell, Ouroboros Praos: an adaptively-secure, semi-synchronous proof-of-stake blockchain, in *Advances in Cryptology – EUROCRYPT 2018, LNCS*, vol. 10821, (Springer, Berlin, Heidelberg, 2018), pp. 66–98
12. J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol: analysis and applications, in *Advances in Cryptology - EUROCRYPT 2015, LNCS*, vol. 9057, (Springer, Berlin, Heidelberg, 2015), pp. 281–310
13. J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol with chains of variable difficulty, in *Advances in Cryptology – CRYPTO 2017, LNCS*, vol. 10401, (Springer, Cham, 2017), pp. 291–323
14. P. Gazi, A. Kiayias, D. Zindros, Proof-of-stake sidechains, in *2019 IEEEE Symposium on Security and Privacy (SP)*, vol. 1 (2019), pp. 677–694
15. A. Kiayias, N. Lamprou, A. Stouka, Proofs of proofs of work with sublinear complexity, in *Financial Cryptography and Data Security*, vol. 9604, (Springer, Cham, 2016), pp. 61–78
16. A. Kiayias, A. Miller, D. Zindros, Non-interactive proofs of proof-of-work, in *Financial Cryptography and Data Security*, vol. 12059, (Springer, Cham, 2020), pp. 505–522
17. A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in *Advances in Cryptology – CRYPTO 2017, LNCS*, vol. 10401, (Springer, Cham, 2017), pp. 357–388
18. I. Shilov, D. Zakoldaev, Multidimensional blockchain and its advantages. Inf. Technol. **26**(6), 360–367 (2020)
19. I. Shilov, D. Zakoldaev, Multidimensional blockchain security analysis. Lect. Notes Netw. Syst. **235**, 911–924 (2022)
20. I. Shilov, D. Zakoldaev, Security of search and verification protocol in multidimensional blockchain. Inform. Autom. **20**(4), 793–819 (2021)
21. I. Shilov, D. Zakoldaev, The robust distributed ledger model for a multidimensional blockchain security analysis. Sci. Tech. J. Inf. Technol. Mech. Opt. **132**(2), 249–255 (2021)
22. Y. Sompolinsky, A. Zohar, Accelerating bitcoin's transaction processing fast money grows on trees, not chains. IACR Cryptology ePrint Archive (2013)

Blockchain Project Workflow Execution for Trustless Operation

Samuel Ashaolu and Lei Chen

1 Introduction

Blockchain was first introduced by a cryptographer in 1992, which was basically utilized as the starting foundation for Bitcoin. Since its inception, the advantages of this technology were not fully maximized and realized until the emergence of Bitcoin [1]. About this time, Bitcoin was regarded and became the largely used form of cryptocurrency relative to blockchain, providing enormous advantages alongside various socioeconomic benefits globally. The blockchain system predominantly provides an incorruptible distributed digital ledger of transactions to automatically store a secured record of financial transactions or virtually everything of value and importance [2]. Traditional contracts have been known over the years to be executed within a centralized system of operation, thus requiring the involvement of a trusted third party. The need of a third party in executing such transactions thereby leads to security, integrity, and reliability issues in traditional contracts. The blockchain technology was created with the notion of resolving and tackling these issues regarding traditional system of contract agreement and eventual execution. Blockchain-based smart contract technology therefore allows untrusted parties to transact together based on predefined conditions without the involvement of third party embedded within the smart contract coding sequence [3]. Blockchain is a distributed ledger that automatically stores all ongoing and previous transactions on the network and thus makes these transactions available to each individual or participants on the peer-to-peer network (P2P). Technological advancement brought about the use of blockchain-based smart contracts for a wide range of applications and usability. Blockchain possesses a range of applications that provides a workable

S. Ashaolu (✉) · L. Chen
Georgia Southern University, Statesboro, GA, USA
e-mail: sa13292@georgiasouthern.edu; LChen@georgiasouthern.edu

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_4

platform to build and develop other decentralized applications hosted on the block. Smart contract is an emerging and yet newer technological concept introduced by cryptographers and engineers to be hosted on the blockchain. Smart contract is a computerized transaction protocol that executes a set of predefined terms and agreements of a contract between untrusted parties on a network [4]. It is a digital signature mechanism capable of executing the release of digital assets, financial agreements, and the automated release of crowd fund which is dependent on the programmed piece of code to all participants involved in this transaction on the network. Comparing traditional contract and smart contract, it is evident that smart contract is independent of a third-party system in contract execution, which would therefore lead to a greater deal of minimal transaction costs [5]. In a workflow management system, each node on the blockchain network has a local Ethereum virtual machine (EVM), which is capable of executing smart contract. Inter-organizational business mechanism could also bring about engagement of two or more organizational participants in an adversarial relationship that requires a need to collaboratively execute a given business project [6]. In this case trust in the required process or project execution could be lacking on the part of the stakeholders [7]. Blockchain technology is able to provide a trust-based platform that is distributed for workflow execution and project monitoring in such situations [8]. A workflow can be described as an organized, systematic, and cyclic process that consists of a series of sequential steps, for example, interactions, algorithms, tasks, and operations among two or more organizations or client with the sole aim and purpose of adding and creating value to the organizations' overall business process [9]. The alignment and integration of organizational business workflow process helps strengthen collaborations. This would improve trust and enable the usability of newer trends of applications across organizations and provide a more secure trading mechanism as well as insurance and notary services [5]. These cogent advantages have, over the years, motivated researchers to dive deeper in developing a blockchain-based business workflow management system model. A couple of challenges still need to be addressed in order to fully maximize the full potential of this technological solution [10]. Blockchain-based smart contract technology is one of the most critical and crucial forms of technology currently driving the acceptance and adoption of blockchain across various private and public sectors globally [4]. The main idea of smart contract was to digitally facilitate an automated system whereby the terms and conditions of a contract between two untrusted entities can be executed in a more secured manner and faster execution time and with contract integrity maintained without dependence of a third-party institution [11]. The working operation of smart contract being an automatic verification machine would grossly reduce intermediaries on the network in contract execution. The matter of trust is based on the code written on the smart contract, which is immutable and unchangeable unless the agreement is met. In addition, the solutions and challenges tackled by smart contract make it undisputable and poised to change, modify, and greatly improve the way business is being executed, controlled, and managed in the twenty-first century and beyond [4]. A blockchain is capable of authenticating a series of blocks that contain various business processes in a cryptographic manner [8]. This makes it difficult to alter the data in the previous block on the chain code without being detected [11]. Within the confines of a distributed blockchain network, participants act independently in order to validate transactions across the chain network and add new block to the chain via data mining, thus replicating the chain across each node [12]. Participants on this chain must agree for validation to transactions on the block, which is referred to as consensus [7]. In workflow management system for project monitoring and execution, it is also imperative that participants across the organizations need to agree on the "state of work," which largely determines the next set of valid activities in the workflow process [6]. Therefore, it is expedient to use blockchain transactions to execute the state of work [11]. This paper thus introduces Blockchain Studio, which is regarded as a novel role-based workflow management system [6]. In this paper, we introduce the blockchain-based smart contract structure mechanism in executing project workflow management system among two or more untrusted parties toward building trust and harnessing the property of the blockchain in data security and smart contract in enforcing the project workflow as agreed by both parties on the network. This paper carefully outlines the applications of smart contracts in solving and mitigating real-life challenges across board [13]. The novelty of this paper was to determine and track the speed and time constraint involved in the usage of smart contract and blockchain as a trustworthy means in project execution management and optimal data-sharing accuracy via Solidity programming computation [14]. It also outlines the deployment of the smart contract on the second-generation and second-target cryptocurrency in the world, namely, Ethereum, which is most suited in the development of decentralized applications (Dapps). On the other hand, traditional contracts would always require the need of a third party for transactional authentication, such as banks, credit loan system, collaterals, insurance company, etc., which would consistently require the need of tons and massive paper works involved as well as a lengthy time process in achieving the desired result and prolonged transaction execution timeline [4]. The Ethereum platform, which greatly provides the best platform in the creation of decentralized applications (dApps), has been understudied to support the overall usage and deployment of smart contract. The remainder of this chapter is structured as follows. Section 2 expounds and provides in-depth illustration of the concept of blockchain technology, the working mechanism of smart contract relative to the facilitation of project workflow execution in a realistic concept [15]. This section also outlines the applications of blockchain-based smart contract in resolving organizational trust issues and proffering workflow layered solutions. Section 3 describes the proposed methodology and architecture of our system and other key concepts. Section 4 describes research results, related work, and a survey research on a broader range of blockchain and smart contract applications. Section 5 discusses blockchain platforms and blockchain as a service (BaaS) and categorizes the blockchain programming languages. Section 6 further describes the conclusion, limitations of our architecture, and future work.

2 Literature Review

2.1 Blockchain and Workflow Operations

The applications of blockchain technology across various sectors have grown at an astronomical rate in the last two decades. Most especially in the technological and financial spaces, blockchain has gained a massive foothold across varying institutions in executing specialized functions [16]. Large corporations and industries are at a faster rate embracing the blockchain technology [5]. Blockchain enables the automation of business workflow process using smart contract, which thus facilitates the intelligent collaboration between trustless entities without the reliance of a centralized authority [9]. Ethereum has been the most prominent blockchain technology to have proposed the design of a decentralized system and a programming language referred to as Solidity, which facilitates the development of smart contracts [16]. Each organizational node participating on the blockchain network has a local EVM with the ability of executing contracts. The blockchain design thus provides a consensus algorithm that provides a trustworthy infrastructure, which allows various partners involved in the organization to collaborate, monitor, perform, and actively audit project workflow transitions [7]. A major challenge of these workflow systems is that they require the continuous exchange of a large proportion of data, which has to be managed off-chain when data is being exchanged between the data producer and consumer alike. This off-chain sharing also requires a high level of security and optimal control in order to follow the workflow execution mechanism. As earlier emphasized, blockchain operates as a data storage capable of storing transactional data, files, etc., whose content is hashed cryptographically represented in hexadecimal values to avoid data breach or a compromise of its data content, which carefully explains its immutability property. Blockchain is a distributed decentralized ledger system [10]. In the blockchain system, the dependency on intermediary institutions is greatly reduced to its barest minimum. Organizations such as banks or any financial institution are completely eliminated, and this due to the fact that transactions are being approved by participants on the network, and this is referred to as a consensus agreement. In the blockchain, the first block is called the "genesis block." Figure 1 shows the blockchain structure and its internal configuration across each block in the chain [17]. Blockchain generally consists of four main elements, asset, ledger, business control network, and cryptographic mechanism, in automatically enforcing the consensus algorithm via participants on the network doing a range of business together [6]. A business network actually consists of individuals and personnel within a company whose core responsibility is to maintain ownership and optimal state of a range of assets [5]. On the other hand, the distributed ledger system in a business network is completely synchronized by the participants in the consensus algorithm [16]. Consensus largely creates a form of compliance among participants in the business process such that each participant agrees on the pattern of information that is being accepted about a given business asset. Provenance is very important as it enables parties on the network to effectively

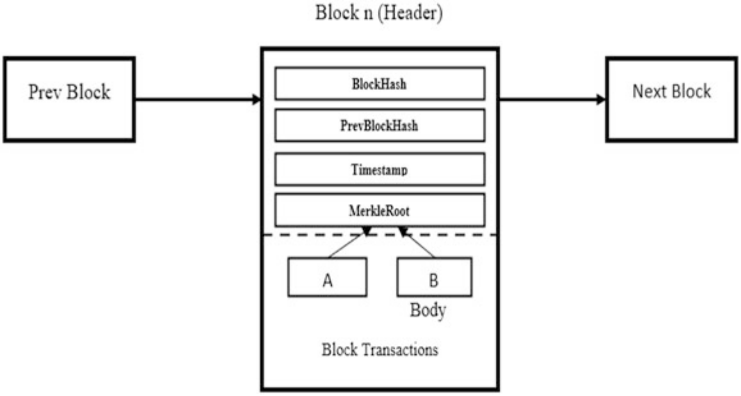


Fig. 1 Demonstration of a chain in blockchain [6]

account for records in a ledger [17]. The immutability property of the blockchain ensures that all records of an asset on the workflow cannot be falsified or tempered. One core advantage in a blockchain application process is the concept of "Shared Ledger"; this is almost similar to data being shared across Google Document whereby authors, viewers, and editors have different levels of privileges across the document in making modifications. In a similar manner, a Shared Blockchain Ledger is similarly updated each time a transaction occurs on the block through a P2P application mechanism. In this case, the ledger is thus updated, distributed, and shared such that there is no centralized control or mechanism controlling the system [8]. Each participant on the network has a duplicate; it is thus permissioned to allow different participants to have complete access to the various segments of the ledger on a timely basis [18]. It is pertinent to note that this is not a duplicated copy of the ledger but a shared copy of all records on the ledger across the network node [7]. Relevant information are only released across the node to participants on a need-to-know basis; this also ensures that transactions are effectively authenticated, secure, and verifiable.

2.2 Salient Features of Blockchain

Some of the most important features that improve the vast reliability and usability of the blockchain technology stem from its applications in various sectors, such as in administrative duties, banking, medical field, etc.

1. *Decentralized*: Blockchain is a decentralized database ledger, and data in this system is stored in a decentralized manner, which helps solve the challenge of data security and accessibility [10].
2. *Open-Source*: Overall, blockchain is generally accessible and therefore participants on the P2P network can access the distributed public records on the ledger, and create distinctive applications using blockchain [7].

3. *Immutable*: Permanently every record is saved in a blocks, and its unchangeable records cannot be modified not until a participant on the network takes over 50% control of the entire system [19].
4. *Autonomy*: In the blockchain setup and during data and information exchange on each respective block, the identities of the participants are limited only to the blockchain address. Thus the information and identities of the participants on the network globally are kept confidential [12].
5. *Auditability*: At some point on the network the ledger is evenly distributed to all participants on the network and each participant thereby has full access to the transactional data available on the system. The identity of each participants stays anonymous to the public. And finally, data on each blocked is converted into a hashing algorithm for security purposes.
6. *Anonymity*: In the blockchain setup and during data and information exchange on each respective block. Identity of participants are limited only to the blockchain address. Thus information and identity of participants on the network globally are kept secret [12].
7. *Security*: The security feature of the blockchain is second to none with a better security. It is almost impossible to shut down the system [3]. Blockchain is heavily immune to hacking due to its complex hashing algorithm to protect data content, and it is secured by a group of computers referred to as nodes, which authenticates the flow of transactions.

2.3 Blockchain Structure

Blockchain, an emerging technology, is regarded as the buildup of blocks in the connecting structures where each of these blocks serves as a form of data storage with the ability to store transactional data [10]. The block basically consists of three things, namely, data, hash, and hash of the previous block as shown in Fig. 2. Metadata can be arranged in three varieties, which include the previous block, in a blockchain system. The value of each block is connected to the hash of the previous block, and this is because the previous block hash is being utilized to frame the content of the new block. It is expedient to note that for each block N, the output is fed into the hash value of the next block assigned N-1. Another block on the chain must be allocated a valid hash, making it part of the network, which is being executed by miners [8].

2.4 Project Workflow Trustless Operation

There are a number of core advantages of blockchain in project workflow management within organizations in providing what is called “Trustless Operation” [9]. In advents of database system failure in managing a project which could result in

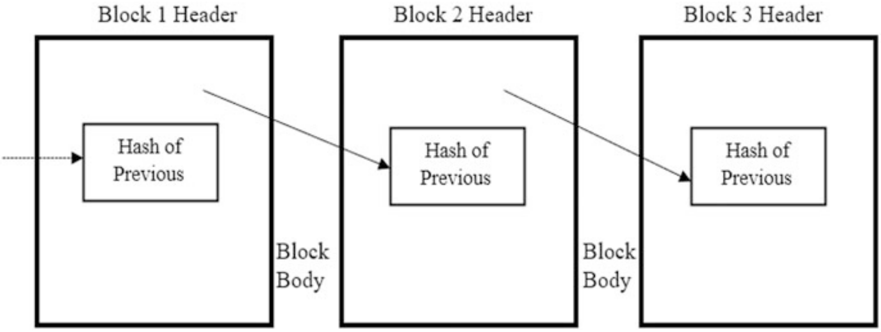


Fig. 2 Structure of a block [7]

system downtime and efficiency of business processes blockchain-based solution can eliminate that downtime by providing a personal copy of project document data to participants in the organization via consensus mechanism thus reducing time delay in the overall project execution. Furthermore, the aforementioned reference made emphasis on the use of Ethereum-based blockchain in the execution of this workflow model, which is suitable for the generation and automation of business workflows. Ethereum blockchains are most suitable in building applications on the blockchain whereby smart contracts can be deployed on these blocks in creating pre-defined codes and agreement to guide the given project [10]. Finally, another new aspect is Blockchain-as-a-Service (BaaS) in business contract operations where each part of the project is updated on the blockchain ledger using smart contract providing truthful visibility to the entirety of a project operation [6].

2.5 Smart Contract and Workflow Project Dynamics

Smart contracts are the predefined rules that automate the execution of a transaction. In workflow project management, the contract for the business process transfer can be embedded in the transaction database [5]. It is this particular code that propels the blockchain to either modify, delete, create, or reorganize the state of a workflow process. A software engineer would think that a transaction quite synonymous to a stored sequential process call on a database [8]. The smart contract is basically a piece of code that runs a series of input parameters that are then being stored as transactions on the blockchain ledger. Smart contracts are mostly programmed in Solidity but can also be programmed in Go or Java script languages. The world is in dire need of trust, and this automated blockchain-based smart contract is able to provide trust in this untrusted digital world [12]. A vast majority of blockchain-based workflow execution systems deploy the use of smart contracts, which has earlier been described as a piece of code stored and deployed on the blockchain and simultaneously executed as part of the blockchain transaction process [20].

A number of blockchain provides a workable platform for the execution of smart contracts such as the Solidity language [21], which was originally developed for the Ethereum blockchain [5]. A project that is executed within the financial ecosystem requires a specified domain workflow implementation, which is based on Ethereum and smart contracts that largely support the digital document workflow relative to the import/export exchange domain [17]. Another important example of domain-specific blockchain workflow management system is in the real-estate ecosystem, which also deploys the use of Ethereum and smart contracts [22]. Another domain is the use of smart contract as choreography monitors in validating workflow messages in controlling the process of sending and receiving messages as well as sending messages according to the process model [23].

2.6 Structure of the Smart Contract in Workflow

Smart contracts can be deployed on three main platforms on a blockchain. One of the most viable and initial platforms is the Bitcoin platform, which is configured to perform cryptocurrency transactions with little or no computing process involved. Another platform is called NXT that is also suitable in developing smart contract. NXT possesses a simplified architecture and is built into the smart contract template. To this end, NXT will only allow the construction and deployment of smart contracts together with those default built-in templates into its system; it however permits various users to customize smart contracts suited to their respective applications and purposes largely due to the absence of coding in its scripting. In addition, the Ethereum platform is the utmost focus of this research. Ethereum supports and makes provision for the development of newer and customized models of the smart contracts as well as the ease in the development of decentralized applications, which is made possible by Solidity language. Ethereum is capable of supporting a wider range of programming functionality [33]. An executable machine or piece of code that guarantees the execution of a contract between two unknown parties is smart contract, which is presented in Fig. 3. The Ethereum platform is used in the development of smart contract. There are still a wide range of technical gaps being associated with the construction and implementation of the smart contract [11].

2.7 Smart Contracts and Traditional Contracts

Contracts were first developed in ancient Rome. Over the years these approaches or styles of contract execution have heavily evolved and developed in complexity and size. Now, they all form the framework and superstructure of modern businesses and trading all across the globe [9]. From time immemorial, traditional contracts have been highly utilized in the execution of terms, agreements, or business contracts of which there has neither been a different approach or perhaps the availability

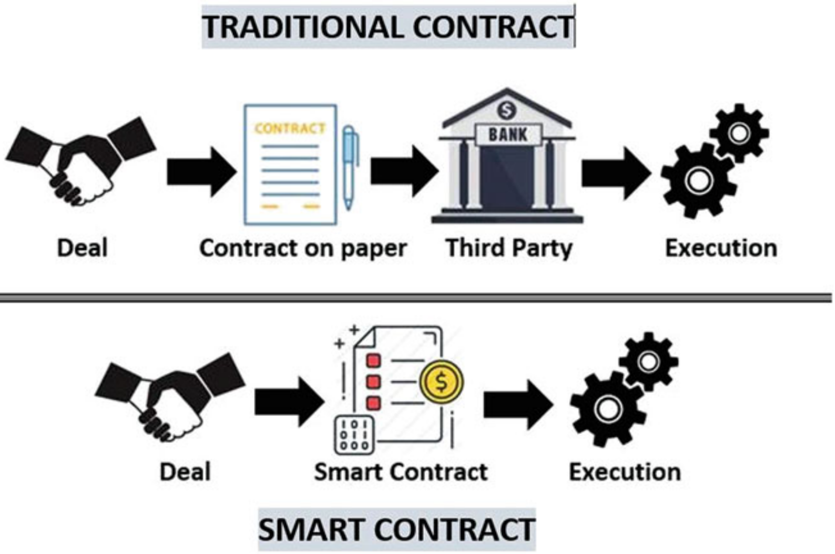


Fig. 3 Comparison of smart and traditional contracts [17]

Table 1 Trade-offs between smart and traditional contracts [12]

	Traditional contract	Smart contract
Intermediaries	Loan agencies	None
Execution timeline	1–2 days	Minutes
Remittance	Manual	Automatic process
Transparency	Unavailable	Available
Archiving	Difficult	Easy
Security	Limited	Cryptographically secure
Cost	Expensive	Cheap
Signature	Manual	Digital signature

of a more reliable, secure, and efficient system in the handling or execution of such contracts [4]. An emerging technology such has the Ethereum-based smart contract being deployed on top of a blockchain has been able to remedy most of the challenges associated with traditional contracts, which is largely in use as shown in Table 1 [17].

2.8 *Smart Contract Applications*

Valentina Gatteshu explained in her article and journal the various applications of Smart Contract, where it can be used and deployed. It is important to note that smart contracts have several real-life applications ranging from the voting system, real estate, law firms, to business outfits. And some of these applications have even already been deployed in Internet of Things (IoT) and real estate property, patents, and online businesses across the globe [4]. The application of IoT alongside blockchain-based smart contracts provides the permission for several nodes on the network to gain full access to various kinds of properties available online and digitally. Another useful application of smart contracts is in the protection of music rights or in the management of music rights [24]. This could become a possibility by storing the legal ownership rights of a patent or copyright work into the blockchain. Here, the immutability property of the blockchain does come handy, such that ownership stored on the blockchain cannot be altered. Smart contract as an automated system plays a huge role in copyright management, making sure the legal owner of such original work gets the required reward for the job done [25]. E-commerce also facilitates online trade between various untrusted parties whereby the smart contract ensures that the agreement between the buyer and seller is enforced without an intermediary third-party involvement [4].

2.9 Advantages of Smart Contracts

1. *Automated*: An automated machine which is self-executing without the need of any manual input [4]
2. *High-Speed*: Smart contracts run on a programmable code thus execution speed is higher than that of traditional contracts [13]
3. *Accuracy*: Based on predefined conditions, the terms and conditions of a smart contract are recorded accurately and cannot be modified [5]
4. *No Intermediaries*: The process is executed without the need of a third party [9]
5. *Secure*: Transactional data is stored in a blockchain decentralized system where data is immutable and unchangeable [6]

2.10 Information and Sharing in Inter-organizational Workflows

From the aforementioned reference topics, the main idea derived from the conceptual framework of each author basically shows how Company A can execute a project with Company B within a project workflow structure and ensure that the project is monitored from initiation until completion using blockchain and smart contract technology [4]. However, different authors used different tools or software in developing this workflow management system such that organizations can collaborate in executing various projects and would be enforced by smart contract [6]. This research relative to IT project management suggests that workflows are required in guiding organizations in managing transactions and confidential data which is a workflow blockchain-based solution via smart contract [3]. Trust has been a major collaboration in business processes that can take the advantages derived from introducing smart contract technology into various business processes [2].

2.11 Blockchain-Smart Contract Workflow Solutions

The solution provided by a blockchain-based smart contract is based on permissioned blockchain, which provides data transparency for all records listed on the ledger for all participants on the node [5]. This mechanism addresses the following project execution challenges in three major steps:

1. *Automates and improves business performance*: Business processes are always executed by workflows. A more efficient workflow, be it physical or digital, usually results in a higher degree of business performance and thus mitigates business capital and running costs [26]. This process is actualized by accurately recording each work project and their corresponding work item as well as their current state on the blockchain [27].
2. *Mitigates company disputes*: The application of blockchain comes in handy here as the issue can be managed by replacing document-based contracts and transforming them into data based contracts [28]. This is actualized by recording each contracts on the ledger, as well each noticeable change request, which includes any form of validation on the blockchain [29].
3. *Improves organizational trust*: Poor information sharing majorly leads to a lack of trust amongst organizations or participants on the network. This further explains the major problems a Blockchain-based Smart Contract aims to tackle and address towards the execution of project workflow amongst participating organizations. Blockchain, via a consensus algorithm, allows the sharing of information to node participants on a need-to-know basis with inbuilt privacy mechanism. The sharing is thus validated, and information can be shared while trust is maintained [30]. These aforementioned steps thus benefit the business partners on the long run across various business functionalities. It hugely enhances better information flow and exchange through contract control and visibility of actionable project steps. It also allows the tokenization of the valuables and improves privacy on the network. Finally, it greatly enhances project process planning, project forecasting, and project performance monitoring and rating to enhance collaboration across untrusted entities [22].

2.12 Project Workflow Execution Layers

To effectively ensure the optimal functionality of workflow execution, there is a cogent need of two main layers: the *coordination layer*, which properly regulates the execution of workflow project and task, and the *authorization layer*, which effectively deploys, maintains, and controls the sequence of data sharing.

1. *Coordination layer*: The execution layer initiates the execution of a task by passing the project details to the executor, which is the needed information. From the coordination layer, once a task is initiated, the coordination layer processes and awaits the result outcome, and based on the results, it continually processes the workflow execution until it reaches the final state in the block. Due to lack of trust among participating organizations, it is equally pertinent to ensure accurate workflow execution [28]. This can be achieved by totally outsourcing the control and management of the coordination layer to a third party in totally controlling the workflow execution process. This nonetheless will come with privacy and security issues [31]. A third-party representative could compromise the data and take full advantage of the confidential data to favor another participating organization, which can expose the whole system to a unique point of failure. A more secure and advanced way of mitigating these trust issues is the implementation of blockchain technology to manage such a collaborative process [23]. Because of the consensus algorithm property of the blockchain, it ensures accurate execution of the smart contract. In light of this, the workflow is thus encoded by a smart contract and therefore executed and validated by the blockchain.

2. *Authorization layer*: The main purpose of the authorization layer is to initiate and deploy a set of authorization to enable the required access to resources on the project. For the authorization layer to be effective, the corresponding conditions have to be satisfied, such as the following: “Temporal authorization, Dynamic resource allocation and least privilege, and Access control enforcement” [12]. The system enables various users to manage and selectively interact with the business rules and predefined agreement as established on the smart contract as the workflows on the ledger. The workflows are usually used as direct inputs to the chain codes or what is termed smart contract, which is a fundamental working functionality of the workflow engine, which is thus implemented on Hyperledger Fabric.

3 Proposed Methodology

An inter-organization business can be modeled in accordance to a workflow, which is composed of a number of activities dependent on the services provided across each organization. The model adopted in this paper is the Blockchain Studio Hyperledger Framework, a novel role-based business workflow management system. The model is then parsed from the Ethereum database platform or back-end, which is then converted into what is called Solidity-based smart contracts before being compiled via the remix and truffle IDE platforms. Solidity code is thus generated from a smart contract algorithm framework. Each project workflow is being assigned a unique code identifier which is then deployed across the Hyperledger blockchain having its terms and agreement enforced by the smart contract [16]. As aforementioned, smart contracts are a set of protocols that are self-executing and embedded with transactional agreements and terms of a contract between the participants on the network [32]. The terms of the contract are programmed on a piece of code, which is then executed on a blockchain-based decentralized platform, and updates the ledger [10]. These agreements facilitate and ensure the eventual negotiations and delivery of digital asset, monetary value, valuable goods and documents as well as items needing a transaction or requiring somewhat exchanged. A blockchain-distributed system platform provides a consensus system in which majority of the participants on the network authorize the transaction, and the identities of the parties are also kept confidential. Figures 4 and 5 thus outline the step-by-step mechanism in the facilitation of this process [5]. This string of code is heavily dependent on the principle of IFTTT (If This Then That). This sort of protocol is the major philosophy embedded in the creation of a smart contract, especially from the coding perspective. Code and conditions are compiled on the Ethereum platform via the EVM. It takes the computer ample time to resolve a cryptographic puzzle, in which this puzzle is being solved using a series of decryption and hashing algorithm. In this process, a newly created block is then merged to the blockchain system, which would be a follow-up to the previous block. Then, a newly created block is thus created and merged to the chain linked to the hash of the previous block. Finally, a new set of data is stored and further encrypted via a process called hashing [17].

Regarding Figs. 4 and 5, the Electronic Official Documents Management System [2] (EODM) embedded on the blockchain network comprises an internal and external communication, which consists of three (3) workflows that aid the processing

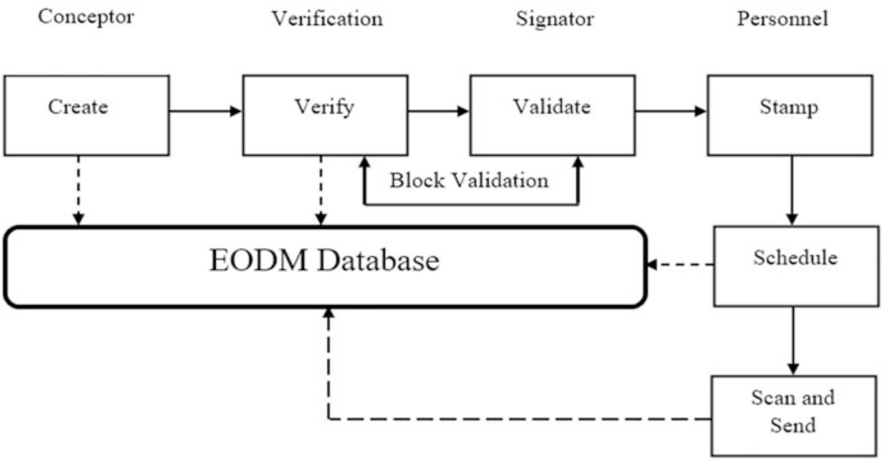


Fig. 4 Dispatching official document workflow for outgoing documents [17]

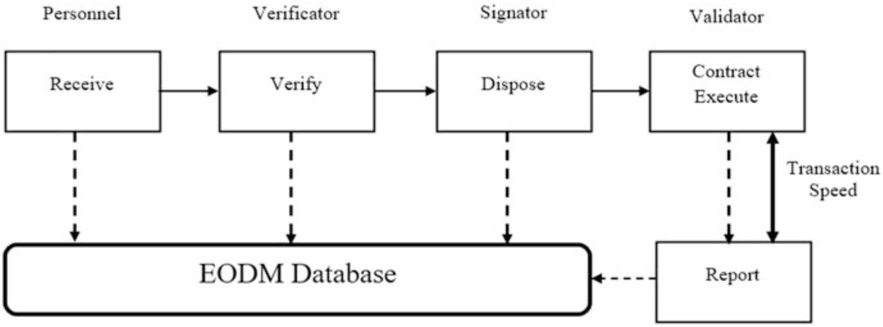


Fig. 5 Dispatching official document workflow for incoming documents [17]

of official projects and documents across the network, which are dispatching, incoming, and disposition workflows [5]. The processes of these documental transfer mechanism are recorded on the node as transactions for document audit trial and tracking [7]. This system is designed with a centralized system to initiate data processing activities stored in the centralized database on the blockchain. The protocols guiding the transfer of such documents for validation are approved and enforced by the smart contract. In the advent of system failure at a particular time period, the activity cycle would be expanded [17]. Dispatching documents is regarded as the process of making, verifying, and digitally validating documents to produce official project and documents for an internal organization [9]. The overall process of dispatching outgoing and incoming documents is presented in Figs. 5 and 6. The documents received are the receipts of official documents from other organizations or partner companies of which validations are checked, scheduled, and forwarded to the relevant officials or participants for disposition to the intended user or client [3]. Outgoing and incoming documents or projects across the blockchain network must first be verified for their validity via a consensus algorithm by the participating organizations. The document details, such as changes, auditing, and cancellation, are recorded, and thus the ledger is updated. On the transactional log, we can ascertain whether the process has followed the regulations enforced by the smart contract [2]. The blockchain ledger consists of the Conceptor, Auditor, Verificator and Signator ledger which performs a profiling function, or an accounting of transactions executed on each block with a timestamp at the execution of a workflow project across organisations who are participants on the network is shown in Fig. 5.

4 Results and Discussions

Based on the results obtained from the execution of a blockchain-based project workflow system for inter-organizational operations, we could deduce that there

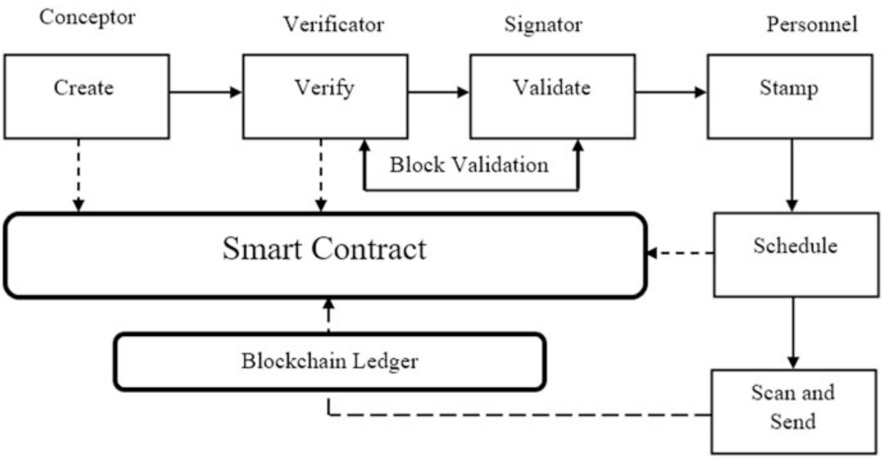
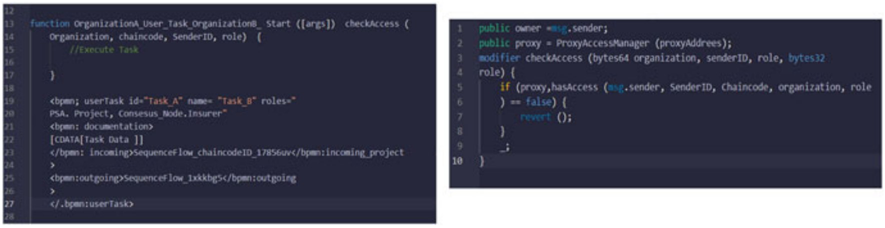


Fig. 6 Workflow of outgoing and incoming documents [17]

exists a comparison between the graphs that shows the distributed blockchain-based EODM proposed project flow management system which increases the activity time efficiency in official business processes in advent of system failures as well as provides the much-needed confidentiality and trust within organizations in project execution. Thus participants can make transactions on the P2P ledger system and increase work efficiency by up to 1.5 times faster in transactional speed, as shown in Fig. 8 [8]. The immutability property of the blockchain provides the platform for workflow and confidential data to be stored on the block, and the workflow is executed by the code agreement set among the participating organization on the network based on a consensus algorithm, as shown in Fig. 7. The blockchain ledger, which consists of the Conceptor, Auditor, Verificator, and Signator ledger that performs a profiling or an accounting of transactions executed on each block with a timestamp at the execution of a workflow project across organizations who are participants on the network. Ethereum has been regarded as the frequently used platform for the development and creation of smart contract [10]. This study is crucial in reducing criminal and theft-based transactions. Figure 8 shows data transfer per second among organizations for incoming and outgoing data transfer with a time difference of about 5 h and approximately 6 h per scenario, respectively, which was better enhanced by the use of smart contract on the blockchain.

4.1 Smart Contracts: Ethereum Platform

In Fig. 9, Nounce is regarded as the counter block that indicates the precise number of transactions being sent from a given account [6]. This is to ensure that transactions are processed no more than once for a single account on the network.



```
function OrganizationA_User_Task_OrganizationB_ Start ([args])  checkAccess (
    Organization, chaincode, SenderID, role)  {
        //Execute Task

    }

    <bpmn; userTask id="Task_A" name= "Task_B" roles="
    PSA. Project, Consesus_Node.Insurer"
    <bpmn: documentation>
    [CDATA[Task Data ]]
    </bpmn: incoming>SequenceFlow_chaincodeID_17856uv</bpmn:incoming_project
    >
    <bpmn:outgoing>SequenceFlow_1xkkbg5</bpmn:outgoing
    >
    </.bpmn:userTask>
```

```
public owner =msg.sender;
public proxy = ProxyAccessManager (proxyAddrees);
modifier checkAccess (bytes64 organization, senderID, role, bytes32
role) {
    if (proxy,hasAccess (msg.sender, SenderID, Chaincode, organization, role
    ) == false) {
        revert ();
    }
    _;
}
```

Fig. 7 Solidity code implementation [9]

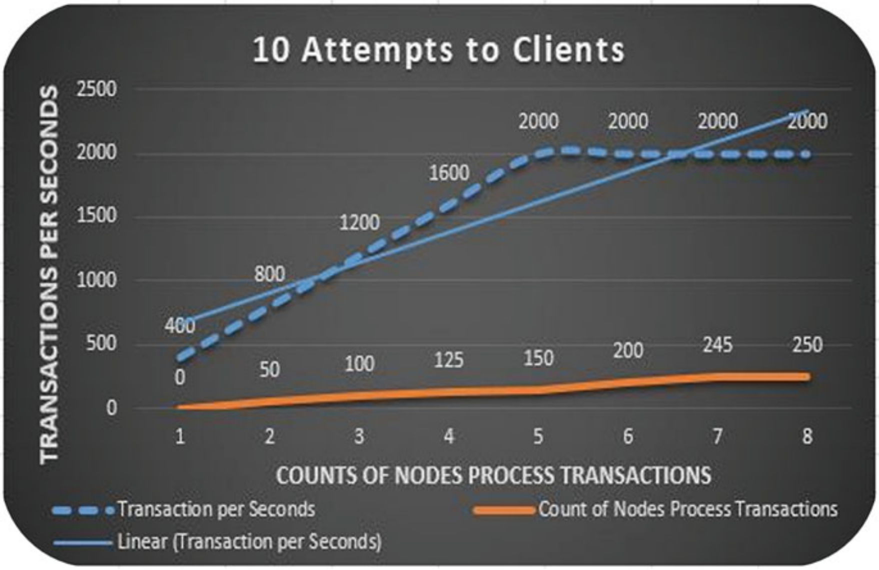


Fig. 8 Transaction speed time in the project workflow execution

The number of wei owned by an account is referred to as the balance block. Wei is defined as a denomination of ETH, and there are 1 × 10^{18} per ETH. CodeHash is defined as the *code* of a particular account on the EVM. The EVM code is automatically executed by the system when the account gets a message call. It is immutable as compared with other account fields [5]. The code fragments of each respective accounts on the platform are contained in the state database encrypted into hashes for easy data collection. This hash value is known as code hash. The storage root block is also referred to as the storage hash, a 256-bit hash of the main node. The storage hash thus encodes or encrypts the storage content of the account, thus making it secure and preventing its data content from being compromised [8].

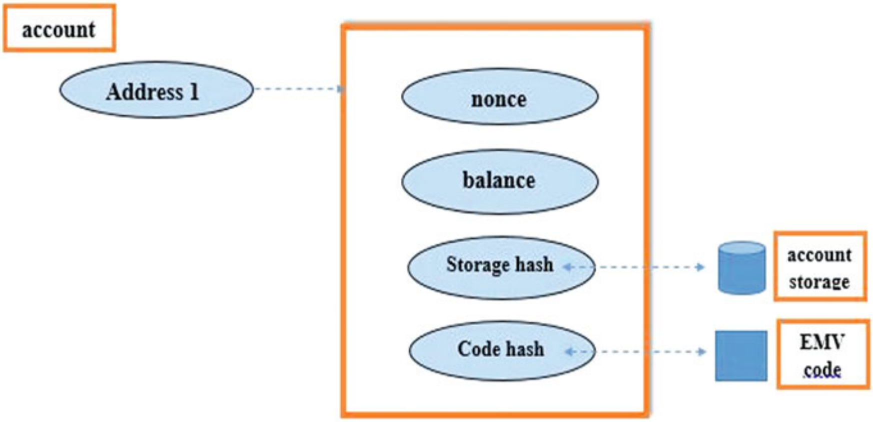


Fig. 9 Ethereum-based smart contract [5]

4.2 Concept of Cryptocurrency

In general and across the globe, cryptocurrencies have greatly provided a technological breakthrough when they emerged from the blockchain technology [17]. Cryptocurrencies are generally referred to as a group of digital currencies. One of the most common examples of cryptocurrency is the Bitcoin. Many other examples of cryptocurrencies, such as the Ethereum, have successively emerged as the second-largest cryptocurrency being used globally [6]. Like smart contracts, Bitcoin also allows a system of digital payments across unknown participants on a network. These parties can be involved in the exchange of digital currency on a secured network without third-party authentication [7]. Ethereum is the second in the world and best blockchain platform that permits the development of decentralized distributed applications (dApps) [8]. Ethereum contributed to the development of smart contracts, which permit the execution of a given contract. Ethereum is a crypto platform built using the Solidity or viper programming language, which enables the swift creation of smart contracts and dApps [5].

4.3 Decentralized Applications (DApps)

DApps are apps that have a decentralized nature or behavior. They are usually free and open-source applications. All their operations and database are cryptographically stored on public blockchains for public accessibility and interaction. Tokens are usually generated for this application, which is being executed by a set of algorithms [5]. These tokens are essential in the optimal usage of these applications, and any contribution to this app receives a token as a contributor to its development. Changes on dApps are made by majority votes. These apps portray a greater tendency to be widely successful in its usage or user-friendliness than even the most successful apps currently trending today due to their flexibility, durability, and transparency [8].

5 Survey Research on Blockchain Applications

5.1 Smart Contract and Blockchain in Food Tracing

The overall goal of the blockchain-based smart contract, which runs on top of the blockchain, is to facilitate, execute, and enforce autonomous verification in an agreement between untrusted parties under predefined conditions without third-party involvement [16]. This paper further outlines the working operation of an Ethereum-based smart contract being deployed on top of a blockchain. The limitations and technical gaps faced in the development of the smart contract technology are also examined in this research. The major key issues identified were security, applications, and performance issues. Metadata can be arranged in three varieties, which include the previous block. In a blockchain, each block is acquired from the previous block; this is because the previous block hash is being utilized to frame the content of the new block. It is expedient to note that for each block N, the output is fed into the hash of the new block N-1. A valid block on the chain must be allocated to a valid hash, making it part of the network that is being executed by miners. One of the main goals of the aforementioned process is to facilitate a successful transaction between two untrusted parties aimed at establishing a contract with predefined terms and conditions. The terms of these contracts developed by a programmer also involves the scripting of this language using the solidity programming language. This string of code is heavily dependent on the principle of IFTTT (If This Then That). This sort of protocol is the major philosophy embedded in the creation of a smart contract, especially from the coding perspective. Code and conditions are compiled on the Ethereum platform via the EVM [19].

5.2 Blockchain in Food Traceability: A Systematic Literature Review

Blockchain technology serves as a major application in improving food quality, inventory tracking, demand response, traceability, transparency, and product recalls for subsidization [33]. There has been a growing interest in blockchain food traceability technology in tracking the quality of food produced for supplier to the final consumer. Several attempts have been made to secure the data being collected across all stages in the distributor chain. The advantages of using the blockchain in food supply chains were also examined in this study. This study investigated about 14 primary recent studies that utilized blockchain in tracking food quality across various points. The 14 blockchain systems studied in this SLR used four different blockchain platforms, and out of these 14 platforms, 8 made use of Ethereum blockchain-based traceability systems, which provided numerous traceability features across each transactional log. The results obtained from the food information traceability tracking report shows that the investigation of this study shows 14 primary studies which were published between 2017 and 2020 from various web sources and digital libraries; 21% of the papers were published in 2017 and 43% in 2020, indicating that the use of blockchain technology in food traceability is gaining the much-needed attention over time [33].

5.3 Blockchain Technology in Supply Chain

Blockchain technology can considerably improve food quality in the food sector via food tracking mechanisms, improve transparency in data sharing, mitigate cost, improve inventory tracking procedures etc. This paper aimed to provide a systematic literature review in tracking food products from all stages of production, from processing, supply, and consumption across the supply chain [34]. The goal of this systematic literature review was to carefully identify and analyze the advantages of using blockchain across the supply chain. This review executed an investigative study on 14 primary recent studies published between 2017 and 2020 involving a pull of web sources and digital libraries. The 14 blockchain system studies in this SLR used about four different blockchain platforms: 8 out of 14 used the Ethereum platform for food-tracing mechanism [5]. According to findings, 21% of the papers were published in 2017 and 43% in 2020, which thus indicates that the use of blockchain technology in food traceability is gaining the much-needed attention [22].

5.4 Towards Automated Migration for Blockchain-Based Decentralized Application

This research aimed to present the underlying structure of the blockchain and smart contract technologies. It also illustrates the various contemporary and emerging applications of the different methodologies used in the smart contracts across various platforms [35]. Smart contracts are a piece of code or machine protocols dependently stored on top of the blockchain network. This piece of code is hosted on a database P2P network. As aforementioned, smart contracts are set of protocols, self-executing, and embedded with the terms and conditions of an agreement between the peers on the network. These terms and conditions are written on a piece of code, which is then executed on a blockchain-based decentralized platform and updates the ledger. This agreement facilitates the exchange of digital asset, money, shares, or property needing a transaction [8]. A blockchain-based decentralized platform provides a democratic system where most of the participants on the network authorize the transaction and the identity of the parties are also kept anonymous. This paper highlights the application of the blockchain in various business sectors like real estate, voting system, E-commerce, and IoT. Results from this research shows that the response time in transactions per second being made by the smart contracts against the processing time was seen to be 1.5 times that of traditional contracts in real-world application [7].

5.5 Ensure Traceability in European Food Supply Chain by Using a Blockchain System

In order to construct a generic agri-food supply chain traceability system which is based on blockchain technology, we adopted a model that aims to implement the farm-to-fork model which is majorly being utilized in the European Union such that various traceability rules and processes can be integrated and executed as a holistic system [34]. This system basically allows food- or health-aware consumers to verify and view product history across the supply chain network from production to destination via the QR code scan. The blockchain implemented in this study is the Hyperledger Sawtooth, which provides permission to legitimate participants on the network. This system employed the Hyperledger Sawtooth platform [16]. This platform was able to generate a traceability application within a generic SC^4. This application had previously been adapted for the management of defined logic through UML. Client communication on the network was created by Sawtooth Validator, REST API, and VN Setting TP in the management of granting permission to participants released by the Hyperledger. The TP application called Agrichain TP aided the validation of the business logic across the entire supply chain. QR code was utilized in viewing product history, and the AES encryption method was deployed for data security [28]. The results obtained from a food information traceability tracking report from the UML diagram in this work was able to obtain a higher software quality in food tracing. All participants and operators on the network were identified across the supply chain, which therefore increases the degree of trust among organizations and health-aware consumers with the involvement of autonomous management of various sequences of activities [27].

5.6 A Proof-of-Concept of Farmer-to-Consumer Food Traceability on Blockchain for Local Communities

The outbreak of the global pandemic presses more importance on the quality of food being produced across the supply-distribution chain from the local farmers to consumers. Considering these, farmers found the need to rely more on middlemen in the sale of produce, which has resulted in price manipulation and lack of communication in providing consumers with reliable food information [36]. This paper incorporates the use of blockchain-based food traceability system eliminating the intermediary, thus allowing farmers to sell their produce to health-aware consumers and able to trace the farming activity of each produce they purchase. This system is based on a private blockchain platform referred to as Hyperledger Fabric, which has an embedded feature of a world state database and a transactional log feature that supports farmers, carriers, and consumers [6]. The farming activities would be recorded by the farmers, whereby the consumers can view the product purchase prior to purchase and track the transportation carriers of that product up until delivery. This is proof-of-concept mechanism on the application of blockchain-based system in agriculture eliminating the need for intermediaries [28]. Three participants are present on this network, namely, farmer, carrier, and consumer, each performing a set of transaction via a web application. The overall results show a system for the farmers to perform farm and shop management processes, and consumers can by products, and carriers are basically responsible for transporting the products embedded in the Hyperledger Fabric framework using the Node.js application API, which interacts with the system and submits transactional log to the network [33].

5.7 Blockchain and IoT-Based Food Traceability for Smart Agriculture

In the last decade, food safety has become a crucial topic worldwide, and tackling these issues has been a daunting task. This paper proposes to examine and design a trusted system that is self-organized as well as open and ecological food traceability system that is based on blockchain and Internet of Things (IoT) technologies [37]. This model involves all parties of a smart agricultural ecosystem not trusting each other. IoT devices were used as a replacement for manual recoding and verification of data. Smart contract was deployed in helping law enforcement agencies process problems quickly. This system employed IoT applications and blockchain technologies, which provides a large amount of benefit to smart agriculture and food traceability [19]. An ad hoc approach solution was used, which involved the use of a traditional ERP (Enterprise Resource Planning) legacy system as well an IoT system allowing the use of smart mobile phones as blockchain node to access data stored on the block. A virtual Trusted Trade Blockchain Network

Cloud Platform (TTBNCP) was relatively utilized to establish a trusted and smart agricultural application system. The results obtained from this system was able to propose a system that made use of blockchain and IoT technologies in building a trusted and smart agricultural system. This was the first attempt to make use of these technologies in food tracing. Results show that the IoT device being used as a replacement for manual recoding and verification of data across the supply chain reduced human intervention to the system much effectively [7].

5.8 A Trustworthy Food Resume Traceability System Based on Blockchain Technology

Ethereum is the most common blockchain platform for developing smart contract. This study is crucial in reducing criminal and theft-based transactions. Technical gaps in smart contract implementation vary from codifying, privacy, and security and performance issues yet to be explored [34]. Ethical gaps in smart contract implementation vary from codifying, privacy, and security and performance issues yet to be explored. Transaction per second was seen to be approx. 1.5 times better while using smart contract than using traditional contracts. The first platform is the Bitcoin: Bitcoin is a public blockchain platform that is used in crypto-currency transactions with a limited computing capability [12]. The second platform is NXT: NXT is another public blockchain platform that includes built-in smart contracts as a template and allows the creation of smart contracts using those pre-installed templates. The third platform is the Ethereum: Ethereum (ETH), which is the focus of this research work, is also a public blockchain platform that can support upgraded smart contracts using the Solidity programming language. The hashing algorithm used on a Bitcoin platform is SHA256, and that on an Ethereum platform is ETHASH. The process of adding a new block to the chain is carried out by miners, in which a certain amount of cryptocurrency is being added to these miners when this cryptographic puzzle is being resolved. Thus, the identity of participants on the network is kept anonymous on the P2P network [31].

5.9 Smart Contract and Blockchain in Food Tracing

There has been a variation of technological trends associated with blockchain technology and the creation of decentralized applications (Dapps) like smart contract implemented on top of a blockchain via Ethereum platform which has facilitated food tracing techniques. The development cycle, security mechanism, and development support were the core foundational models utilized in the development of smart contracts. It also addresses the technical pitfalls, elemental components, and future implementation of this model in smart contract build-up. Ethereum and the EVM with the Solidity programming language are the core platforms used in the development of the smart contract and other Dapps [12]. A systematic mapping method was used for data extraction and the mapping process in this research aimed at identifying and gathering previous or past research papers on the development of smart contract via the blockchain technology on the Ethereum platform. Systematic mapping involves search process and searching of paper in building a strong research outcome. An essential pitfall in the development of smart contract on Ethereum was seen to be security vulnerability threat and exposure. A step to combat this issue proffered the need for code development designed to address the vulnerability of contract exposure [33].

5.10 Blockchain Technologies and Their Applications in Data Science and Cyber Security

Highlighted in this paper are the core essential applications of blockchain technology. It provides a basis for which these applications are expedient in the field of data science and cyber security. It explores and examines the various data science methods and techniques involved in the transactional process of blockchain [34]. Technical concepts such as blocks, smart contract, Bitcoin cryptographic checksum, and blocks were extensively discussed relative to the operation of blockchain for data science and cyber security purposes. Data analytics and data sharing process are key in blockchain technologies providing security for data life cycle, IoT, and DDoS attacks [37]. The Hyperledger Fabric blockchain process was utilized in analyzing the systemic approach of how the blockchain can be used to process Big Data analytics in analyzing private data. Data security and data privacy were key elements that transcend all aspects of data science, and this blockchain technique was used to provide solutions due to the decentralized infrastructure property of the blockchain. Computed graphs from the blockchain were used to predict Bitcoin price dynamics through data science and data analytics. It was proven that the blockchain technology was able to provide maximum security in the entire data lifecycle process involving data collection and analysis [16].

5.11 Towards Automated Migration for Blockchain-Based Decentralized Application

This paper utilized a systematic literature mapping (SLM) approach aimed at investigating the technological advancement and current practices regarding blockchain-based applications in supply chain management (SCM). These applications were critically analyzed based on the business industrial sector, utilized blockchain framework, and prevailing challenges. This research provides a careful outline of the various blockchain use case as it relates to supply chain management [12]. A five-step systematic mapping process was designed based on pre-existing research work related to a blockchain-based applications of supply chain management. Scopus electronic database was used to gather quality research papers using the search query “Blockchain” and “Smart Contract” and “Supply Chain Management.” To ensure high-quality survey papers, the inclusion and exclusion criteria were utilized using a series of hypothetical questions. Analysis results show that a vast number of the blockchain solutions and industrial applications were being developed for the agricultural and food industry followed by the pharmaceutical and other health related sectors which are equally important [13]. The solution seemed satisfactory and reliable when these applications were built on Ethereum and Hyperledger Fabric frameworks [22].

5.12 Rebuilding Food Supply Chain with the Introduction of Decentralized Credit Mechanism

This paper introduces the concept of credit management system in a bid to further improve the security architecture of the information traceability tracking software built on the blockchain [9]. The design of the RFID traceability system is developed

Table 2 Blockchain platforms and BaaS platform – *Blockchain as a Service (BaaS)* [34]

BaaS platform	Use cases	BaaS platform	Use cases
Azure	Supply chain	Corda	Financial markets, digital assets, digital identity, energy, government, etc.
AWS	Supply chain, letter of credit, system-of-record, trading and asset transfer, retail	Crypto APIs	Gas fee management, tokenization solutions, crypto wallet, and lending
IBM	Banking and financial markets, government, healthcare, insurance, services, supply chain	Nexledger	Financial markets, trade financing, audit, and regulatory compliance, insurances
Oracle	Supply chain, voting, banking, financial markets, and payments	Blockchain Service BCS	Supply chain, notarization for crowdfunding, digital assets
Alibaba	Supply chain, digital content ownership, anti-counterfeiting Service	BLOCKO	Financial security insurance, government, supply chain
SAP	Supply chain, identity management	SAP	Financial markets, manufacturing, healthcare
Kaleido	Financial markets, supply chain, letter of credit, healthcare	Baidu	IoT, hazardous chemical logistics, financial collection
Rubix	Supply chain		

Table 3 BaaS platforms and programming languages – *Blockchain as a Service (BaaS)* [34]

BaaS platform	Programming language	BaaS platform	Programming languages
Azure	Solidity, Serpent, Go, Java, Kotlin, JavaScript	Baidu	Solidity, Serpent, Go, Java
AWS	Solidity, Serpent, Go, Java, Kotlin	Google	Solidity, Serpent, Go, Java
IBM	Go, Java, Node.js, JavaScript, TypeScript	Chainstack	Go, Java
Oracle	Go, Java, TypeScript	Corda	Kotlin, Java
Mission Critical	Solidity, Serpent, Kotlin	Kaleido	Solidity, Serpent, Kotlin
SAP	Go, Java	Rubix	Solidity, Serpent

to solve problems related to data tampering and data security, especially in the agricultural sector for food tracking mechanisms. Based on blockchain, a new decentralized credit system would be implemented for enhanced security and reduction in time and cost, thereby providing a means of authentication during the tracking of food across various middlemen [13]. The Credit Management System Model on a blockchain is broadly divided into four layers for complete implementation; "traceability entity layer, Internet of Things (IoT) layer, blockchain and the credit entity layers". The traceability entity layer serves as the main core layer for the food supply chain structure while the IoT layer collects data on the supply chain feeding this data to the blockchain layer. The blockchain layer records transactions and credit data on the ledger via consensus algorithm to execute the credit management system [34]. From a theoretical and practical perspective, the results obtained from a food information traceability tracking report with the introduction of the credit management system show that the members of the blockchain (Tables 2 and 3).

6 Conclusion

Blockchain differs in its architecture from other traditional centralized databases in that blockchain possesses salient properties and unique characteristics, making it the most recent and upgraded version of traditional centralized databases. Blockchain is a decentralized distributed database in that it is able store data, that is, transactional data on its database [9]. These data are non-tamperable, immutable, and traceable, which is jointly managed and maintained by multiple parties or members via a consensus algorithm on the network [19]. Each participant on the network must agree upon a consensus on an updated data ledger based on pre-defined rules enforced by the smart contract being deployed on the blockchain network. Based on the results that described the implementation of a blockchain based-project workflow for trustless operation, this paper has been able to illustrate a mechanism of project execution and workflow agreement among participating organizations in executing "Trustless Operation" on the blockchain, which avoids data falsification or tampering and preserves the integrity of workflow project execution among untrusted party [9]. The final results show that the proposed blockchain-based system is more profitable than the previous system. Overall, the system shows an increasing activity time efficiency for various business processes [17]. Technical gaps were found in the design and technical buildup of the smart contract requiring attention for future studies. Technical gaps range from codifying, security, privacy, and performance [7]. Ethereum-based smart contracts was discovered to have technical issues ranging with scalability, runtime, power consumption from mining exercise. In addition, future work should examine the transition of an Ethereum-based smart contract from [7] "Proof-of-Work to Proof-of Stake," thus enhancing processing time in the addition of blocks to the chain and reducing power consumption in its overall computing [8].

References

1. C. Rondanini, B. Carminati, F. Daidone, E. Ferrari, Blockchain-based controlled information sharing in inter-organizational workflows, in *2020 IEEE International Conference on Services Computing (SCC)* (2020), pp. 378–385. https://doi.org/10.1109/SCC49832.2020.00056
2. N. Bore et al., On using blockchain based workflows, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2019), pp. 112–116. https://doi.org/10.1109/BLOC.2019.8751446
3. J. Evermann, Adapting workflow management systems to BFT blockchains – the YAWL example, in *2020 IEEE 24th International Enterprise Distributed Object Computing Workshop (EDOCW)* (2020), pp. 27–36. https://doi.org/10.1109/EDOCW49879.2020.00017
4. L. Mercenne, K. Brousmiche, E.B. Hamida, Blockchain studio: a role-based business workflows management system, in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (2018), pp. 1215–1220. https://doi.org/10.1109/IEMCON.2018.8614879
5. Y. Chen, Blockchain in enterprise: an innovative management scheme utilizing smart contract, in *2020 9th International Conference on Industrial Technology and Management (ICITM)* (2020), pp. 21–24. https://doi.org/10.1109/ICITM48982.2020.9080356
6. L.X. Downey, F. Bauchot, J. Röling, Blockchain for business value: a contract and work flow management to reduce disputes pilot project. IEEE Eng. Manage. Rev. **46**(4), 86–93, Fourth quarter (2018). https://doi.org/10.1109/EMR.2018.2883328
7. X. Liu, A smart book management system based on blockchain platform, in *2019 International Conference on Communications*, Information System and Computer Engineering (CISCE) (2019), pp. 120–123. https://doi.org/10.1109/CISCE.2019.00035.
8. S. Choudhari, S. Das, S. Parasher, D. Gangwar, Sub contractor life cycle management in enterprise system using blockchain technology, in *2021 6th International Conference for Convergence in Technology (I2CT)* (2021), pp. 1–7. https://doi.org/10.1109/I2CT51068.2021.9417981
9. B. Carminati, C. Rondanini, E. Ferrari, Confidential business process execution on blockchain, in *2018 IEEE International Conference on Web Services (ICWS)* (2018), pp. 58–65. https://doi.org/10.1109/ICWS.2018.00015
10. I.G.B.B. Nugraha, Y. Bandung, A. Zaky, Official document management for government service in Indonesia using smart contract, in *2019 IEEE International Smart Cities Conference (ISC2)* (2019), pp. 390–395. https://doi.org/10.1109/ISC246665.2019.9071643

11. K. Tsoulias, G. Palaiokrassas, G. Fragkos, A. Litke, T.A. Varvarigou, A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems. IEEE Access **8**, 130952–130965 (2020). https://doi.org/10.1109/ACCESS.2020.3006383
12. S. Khan, M. Al-Amin, H. Hossain, N. Noor, M.W. Sadik, A pragmatical study on blockchain empowered decentralized application development platform, in *Proceedings of the International Conference on Computing Advancements ICCA 2020*, Association for Computing Machinery, New York (2020), Article 82, pp. 1–9. https://doi.org/10.1145/3377049.3377136
13. A. Mendi, T. Erol, E. Safak, T. Kaym, A blockchain smart contract application framework, in *2019 International Symposium on Networks*, Computers and Communications (ISNCC) (2019), pp. 1–4. https://doi.org/10.1109/ISNCC.2019.8909194
14. C. Mooney, The truth about, Sci. Am. (2011), pp. 80–85. Nick Szabo, The idea of smart contracts (2018). [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html. Accessed 31 Mar 2018
15. R.G. Brown, J. Carlyle, I. Grigg, M. Hearn, Corda: an introduction (2016), pp. 1–15
16. G. Zou, Y. Xue, Application of blockchain technology in credit management for credit bank system, in *Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering (EITCE 2020)*, Association for Computing Machinery, New York (2020), pp. 62–66. https://doi.org/10.1145/3443467.3443729.
17. G. D'mello, H. González-Vélez, Distributed software dependency management using blockchain, in *2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)* (2019), pp. 132–139. https://doi.org/10.1109/EMPDP.2019.8671614
18. C. Cachin et al., Hyperledger fabric (2018), pp. 1–15. K. Wust, A. Gervais, Do you need a blockchain?, in *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, no. i (2018), pp. 45–54
19. M. Abdelhamid, G. Hassan, Blockchain and smart contracts, in *Proceedings of the 2019 8th International Conference on Software and Information Engineering (ICSIE'19)*, Association for Computing Machinery, New York (2019), pp. 91–95. https://doi.org/10.1145/3328833.3328857
20. Hyperledger, Hyperledger projects - Hyperledger (2018). [Online]. Available: https://www.hyperledger.org/projects. Accessed 18 June 2018
21. G. Eason, B. Noble, I.N. Sneddon, On certain integrals of Lipschitz-Hankel type involving products of Bessel functions. Phil. Trans. Roy. Soc. London **A247**, 529–551 (1955)
22. A. Abuhashim, C.C. Tan, Smart contract designs on blockchain applications, in *2020 IEEE Symposium on Computers and Communications (ISCC)* (2020), pp. 1–4. https://doi.org/10.1109/ISCC50000.2020.9219622
23. M. Westerkamp, Verifiable smart contract portability, in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2019), pp. 1–9. https://doi.org/10.1109/BLOC.2019.8751335
24. I.S. Jacobs, C.P. Bean, Fine particles, thin films and exchange anisotropy, in *Magnetism*, ed. by G. T. Rado, H. Suhl, vol. III, (Academic, New York, 1963), pp. 271–350
25. Y. Yorozu, M. Hirano, K. Oka, Y. Tagawa, Electron spectroscopy studies on magneto-optical media and plastic substrate interface. IEEE Transl. J. Magn. Jpn **2**, 740–741 (1987)
26. GARTNER, Top 10 mistakes in enterprise blockchain projects - Smarter with Gartner. [Online]. Available: https://www.gartner.com/smarterwithgartner/top-10-mistakes-inenterprise-blockchain-projects/. Accessed 08 Mar 2019
27. C. Cachin, Architecture of the hyperledger blockchain fabric, in *Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers*. Semanticscholar (2016).
28. Mike Hearn, Smart property - Bitcoin Wiki (2018). [Online]. Available: https://en.bitcoin.it/wiki/Smart_Property. Accessed 31 Mar 2018. G.W. Founder, E. Gavin, Ethereum: a secure decentralised generalised transaction ledger (2017), pp. 1–32

29. Derar E., Amma E., A survey paper on blockchain as a service platforms. Int. J. High Perform. Comput. Netw. Accessed Oct 2021
30. J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, vol 2, 3rd edn. (Clarendon, Oxford, 1892), pp. 68–73
31. D. Liang Xi, B. Frederic, R. Jos, Blockchain for business value: a contract and workflow management to reduce disputes pilot project. IEEE Eng. Manage. Rev. **46**(4), Fourth Quarter (2018)
32. E. Derar, E. Amna, A survey paper on blockchain as a service platform. Int. J. High Perform. Comput. Netw. **17**, 8–18 (2021))
33. R. Richard, H. Prabowo, A. Trisetyarso, B. Soewito, Smart contract development model and the future of blockchain technology, in *2020 the 3rd International Conference on Blockchain Technology and Applications (ICBTA 2020)*, Association for Computing Machinery, New York (2020), pp. 34–39. https://doi.org/10.1145/3446983.3446994
34. Y.-J.J. Kuo, J.-C. Shieh, Cross-domain design of blockchain smart contract for library and healthcare privacy, in *Proceedings of the 4th International Conference on Medical and Health Informatics (ICMHI 2020)*, Association for Computing Machinery, New York (2020), pp. 122–126. https://doi.org/10.1145/3418094.34
35. Gartner, (2017). [Online]. Available: https://www.gartner.com/smarterwithgartner/top-trends-in-thegartner-hype-cycle-for-emerging-technologies-2017/. Accessed 21 July 2018
36. S.J. Pee, E.S. Kang, J.G. Song, J.W. Jang, Blockchain based smart energy trading platform using smart contract, in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (2019), pp. 322–325. https://doi.org/10.1109/ICAIIC.2019.8668978
37. M. Alharby, A. Aldweesh, A. van Moorsel, Blockchain-based smart contracts: a systematic mapping study of academic research, in *2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB)* (2018), pp. 1–6. https://doi.org/10.1109/ICCBB.2018.8756390

Part II
Blockchains in Internet of Things and Mobile Phones

Protecting Location Privacy in Blockchain-Based Mobile Internet of Things

Abdur R. Shahid, Niki Pissinou, and Sajedul Talukder

1 Introduction

The Internet of Things, or IoT, is a network of interconnected computing devices that use unique identifiers (UIDs) to facilitate communication between devices and the cloud, as well as among themselves. Thanks to low-cost computers, the cloud, big data, analytics, and mobile technologies, IoT has emerged as one of the most important technologies of the twenty-first century in recent years. A variation of IoT is the mobility-centric IoT, which unifies the sensing ability with the mobility of the devices. The core component of such mobility-centric IoT systems is the location information of the IoT devices: users share their location information through their devices with a system to get a variety of location-based services (LBSs). Formally, location-based services are “services accessible with mobile devices through the mobile network and utilizing the ability to make use of the location of the terminals.” The location information of the users, for example, has made location-based recommendation systems a standard part of our daily life. Real-time navigation systems, intelligent vehicle systems, crowdsensing, indoor navigation for blind people, and health monitoring are just a very few examples of location-based services which are benefited from the mobility aspect of IoT. From an economic perspective, mobility-centric IoT has a tremendous impact on the overall GDP. As

A. R. Shahid (✉)
Robert Morris University, Moon Twp, PA, USA
e-mail: shahid@rmu.edu

N. Pissinou
Florida International University, Miami, FL, USA
e-mail: pissinou@fiu.edu

S. Talukder
Southern Illinois University, Carbondale, IL, USA
e-mail: sajedul.talukder@siu.edu

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_5

IoT devices create, analyze, and share massive volumes of security-critical and privacy-sensitive data, they are potential targets for a variety of attacks, including location privacy attacks. Moving objects, geographical coordinates, present time, and distinctive properties distinguish location data from other data, which is discrete and valuable. Location privacy is an essential aspect of the Internet of Things privacy protection. It mainly relates to the location privacy of each node in the Internet of Things, as well as the location privacy of the Internet of Things in providing various location services, such as RFID reader location privacy, RFID user location privacy, sensor Node location privacy, and location-based privacy issues based on location services [1].

As of this writing, the mobility-centric Internet of Things (IoT) systems utilize a centralized model to handle the vast amount of data generated by IoT devices (e.g., smart vehicles in the Vehicular Ad Hoc Network (VANET) [2], smartphones in ad hoc networking-based mobile crowdsensing [3]). Such models are weak in ensuring security and trust and are not capable of handling the fast-paced growth of IoT. Thus, distributed systems are considered to address the problems of IoT systems. Recently, blockchain, a unique distributed technique, has gained tremendous attention from the IoT community [4–8]. A blockchain is a distributed ledger that uses cryptographic protocols to allow peer-to-peer data transfer and storage [9, 10]. It provides built-in integrity of information and security of immutability by design, making it very useful for ensuring trust, security, and transparency in P2P trustless networks. There are two basic types of blockchain architectures based on the permissions of the users to read/write on the ledger: permissionless and permissioned. Permissionless blockchains are generally public blockchains where anyone may read, write, and participate in consensus. Permissionless blockchains have a high level of decentralization since they can accommodate more users and span a much broader network. Permissionless blockchains are often open source, meaning that they are developed by a community and may be modified and used by anybody. Because the users must maintain some kind of anonymity, permissionless blockchains are far more transparent. Transactions are encrypted using different cryptographic methods, and wallet addresses cannot typically be linked back to blockchain users. A permissionless blockchain eliminates the necessity for two nodes or participants to verify each other's validity. As a result, permissionless blockchains are more secure in general, as the risk of bad actors in the network colluding is decreased. Permissionless blockchains, on the other hand, suffer from several problems, including privacy concerns, lower TPS, scalability issues, and high energy consumption, owing to transaction verification and proof of work.

Similar to many other fields, permissioned blockchain is also being studied in the IoT of mobile devices. For better understanding, we draw the motivation of a permissioned blockchain from CreditCoin, a privacy-preserving blockchain framework for the Vehicular Ad Hoc Network (VANET) [11]. In this framework, the vehicles are required to be registered with the authority. This authority is responsible for generating and providing the vehicles with cryptographic keys and keeping track of the relationship between the vehicles and the provided keys. A set of trace managers at different locations also aids the authority in tracking malicious vehicles/users. In this framework, only road-side units (RSUs), and authorized vehicles are responsible for managing the blockchain. This framework is built around the short-range communication technology-based P2P network of vehicles. Here, the vehicles make transactions with their peers such that each transaction is signed by each of the peer vehicles by their public keys. As these transactions are made through a short-range communication technology (e.g., Wi-Fi, Bluetooth), they can be treated as a proof of location (PoL) for the vehicles' whereabouts in the spatiotemporal domain. In some frameworks, such as the one proposed in [12], the proof of location is explicitly defined in the design. Based on the transaction information, the vehicles generate a rating about each other and forward them to the nearest RSU. The RSUs then compute the overall rating of each vehicle and append the new rating into the blockchain. Similar motivation can also be drawn from the work presented in [13]. Obviously, these frameworks can be integrated into many other mobility-centric IoT scenarios, such as mobile crowdsensing.

Mobile IoT devices create, analyze, and share massive volumes of location-centric privacy-sensitive data, they are potential targets for a variety of attacks, including location privacy attacks. Geographical coordinates, present time, and distinctive properties distinguish location data from other data, which is discrete and valuable. Location privacy is an essential aspect of the IoT privacy protection [1, 14–16]. In a centralized architecture of IoT, all the location-based data are stored on the cloud. In a blockchain system, the transactions carry the location information. In both permissionless and permissioned blockchains, these location-based transactions can be analyzed to infer location-centric privacy-sensitive information. However, in a permissionless blockchain, a mobile IoT node can change its key pairs frequently and hence protect its location privacy. On the contrary, on a permissioned blockchain, IoT devices do not enjoy such privilege, as the key distribution is handled by a blockchain authority. The objectives of our work are as follows:

- Provide a formal definition of the location privacy-invading problem in the context of permissioned blockchain.
- Present a solution to protect location privacy in permissioned blockchain.

Against this backdrop, in this chapter, we study the location privacy issue in the context of permissioned blockchain, where:

- The authority of the blockchain holds the public and privacy key distribution task in the system.
- A transaction can be considered as a proof of location (PoL) for a user's temporal whereabouts.
- There is a spatiotemporal correlation between the locations.

We make the following key contributions:

1. We first discuss the limitations of existing location privacy-preserving mechanisms under a PoL in the context of permissioned blockchain.
2. We present an effective solution, called **BlockPriv**. As discussed above, in **BlockPriv**, the worst form of privacy leakage is considered. That is, whenever

Table 1 Notations and their description

Notation	Description
MU	Mobile user or mobile node
$\mathcal{N}_x$	Privacy parameter for a location l_x
$\mathcal{P}(l_h)$	Privacy level achieved for location l_h
$Pr^t_{MU}(l)$	MU's probability of being at location l at time t
l^s	A sensitive location
S	Set of all sensitive locations of a MU
$\mathcal{U}(l)$	Loss of utility for location l
T_r	A trajectory
n	Total number of sensitive locations in a T_r
δt	Time difference
$\mathcal{L}_a$	Set of all locations reachable to/from location l_a
$\Phi(a, b)$	Required time to reach from location l_a to l_b
$\|X\|$	Size/number of elements in a set X
α	% of location types selected as sensitive
r	Privacy region radius

an IoT node makes a transaction with its peers, its location information is known to the malicious blockchain authority, and the authority is completely capable of mapping the real identity of a node with its public key pairs. Taking a node's privacy preference for different locations and spatiotemporal correlation between the transactions, **BlockPriv** decides whether or not a node should make a transaction, such that its undisclosed sensitive location's privacy is also preserved with a set of locations.

3. We quantify the trade-off between privacy and utility theoretically and empirically using two factual datasets.

The rest of the chapter is organized as follows. Related works are discussed in Sect. 2. The overview of the system and its design goals are presented in Sect. 3. Then, the proposed **BlockPriv** approach is detailed in Sect. 4. Important security, privacy, and utility aspects of **BlockPriv** are analyzed in Sect. 5. A discussion of the experimental analysis is covered by Sect. 6. Finally, the chapter is concluded in Sect. 7. Important notations used in the chapter are presented in Table 1.

2 Related Work

Location privacy preservation is a comparatively well-studied problem in centralized architecture-centric IoT systems. Several classes of mechanisms have been proposed to mitigate the privacy leakage, such as:

1. Pseudonym
2. Location perturbations
3. Spatial obfuscation

The goal of these mechanisms is to apply them to a node's actual location before releasing it to the central authority. For instance, in the case of a pseudonym, before revealing the location, the mechanism changes the ID of a node to make it untraceable [17]. These approaches depend on a trusted third party (TTP) to carry out the steps of changing pseudonyms. This is similar to the mixing approach [18] used in blockchain to improve privacy by exchanging the public key of a mobile node with a random public key such that the probability of linking multiple transactions is reduced. However, in a permissioned version of the blockchain, such an approach will not work.

Perturbation mechanisms, such as differential privacy-based geo-indistinguishability [19], add statistical noise to a node's real location before it is shared with the system. Obviously, under a PoL, such mechanisms have limited impact [20]. On the other hand, spatial obfuscation reduces the precision of the actual location information before releasing it to the authority of the system. This is done by either infusing more locations [21] or replacing the actual location with a realistic larger region [22]. Similar to location perturbation, location obfuscation works only at a limited scale under the PoL. In a nutshell, the existing privacy-preserving mechanisms, designed for centralized IoT systems, cannot be applied in a plug-and-play way to the problem that we are trying to solve here.

In the scope of blockchain, the frequent change of public keys is the most explored solution to preserve privacy [9, 23–25]. It was first proposed by Nakamoto [9], the creator of Bitcoin. Motivated by Bitcoin's solution, Dorri et al. [24] also suggested using a fresh unique public key to prevent linkage attacks while communicating with other nodes in their proposed Lightweight Scalable Blockchain (LSB) architecture for smart vehicle ecosystems. In blockchain-based centralized proof-of-location (PoL) generation, Brambilla et al. [26] also proposed changing the public keys frequently to preserve a node's sensitive location privacy while generating proof of locations. Michelin et al. [20] proposed a privacy-preserving blockchain-based SpeedyChain framework for a vehicular network scenario. Similar to most of the other works in this context, SpeedyChain considers the fixed positioned roadside infrastructure units (RSUs) as the key to maintaining the blockchain. Unlike Bitcoin or Ethereum-like blockchains, here, for each vehicle, there exists exactly one block in the blockchain. In order to maintain privacy, this framework proposes the timely change of the public key of each vehicle. However, these frameworks do not fit completely into the scenario considered in this chapter, where the authority of the blockchain controls the private and public key distributions to the mobile nodes in the system.

The idea of a permissioned blockchain primarily stemmed from the evidence of misuse of freedom in public blockchains for illegal activities. For instance, almost half of the bitcoin transactions are estimated to be related to illegal drug sales, ransomware, and other malicious activities [27]. Hence, the deanonymization of blockchain users has gained significant attention from both law enforcement and the security and privacy communities. In fact, it is found that changing the public keys in order to nullify a linking attack in a public blockchain is not quite as bulletproof as it was expected [28, 29]. Research efforts show that it is possible to map the public keys of Bitcoin users to their unique identities (e.g., IP addresses) [28, 29]. For instance, Koshy et al. [28] were able to deanonymize 1162 addresses by analyzing transaction relaying patterns. Biryukov et al. [29] proposed a deanonymizing algorithm by exploiting only the input and output transactions of mixing services and identified a relationship between the input and output addresses at very high accuracy. Recently, Roulin et al. [30] applied decision tree algorithms on smart home devices' data (e.g., smart things, nest smoke alarm) by utilizing off-chain information to classify IoT devices for understanding a user's activity pattern. While the work is done in the context of a smart home, it can be adapted for the mobility of IoT devices. All these deanonymization works highlight that simply changing the public keys frequently is not the ultimate solution to providing privacy in the blockchain, even in a public version.

Moving forward, our work is focused on an authority-based permissioned blockchain where privacy is tougher to achieve by default. It is closely related to the work proposed by Li et al. [11] in the context of a vehicular network. Using their proposed framework, it is possible to achieve only conditional privacy, as the trace manager can track anyone at any time, if necessary. Similarly, Yang et al. [13] presented a blockchain-based decentralized trust management framework for vehicles where each vehicle is registered with the system using its VIN number. Thus, only conditional privacy can be attained with this framework. Likewise, Sharma et al. [31] proposed a permissioned blockchain by incorporating traceability features while maintaining privacy on the Internet of Vehicles (IoV). However, they used a server for vehicle registration, which would store all vehicle IDs in an encrypted scheme; the central authority can track any vehicle when needed.

To achieve complete location privacy, Yang et al. [32] proposed an obfuscation approach to protect location privacy in a private blockchain for crowdsensing applications. In this work, a worker submits an obfuscated region to the system to protect their exact location's privacy. However, in the case of P2P communication of the nodes, this type of approach cannot be applied without the collaboration of the nodes. Jia et al. [33] designed a blockchain-based incentive mechanism for crowdsensing applications with a focus on preserving the location privacy of the users. In their framework, a confusion layer was proposed, in which a user's location is encoded in such a way that it can be confused with other $k - 1$ users' locations. While this could be a solution to protect location privacy, it requires the honest collaboration of other users.

In contrast to all these works, we intend to design a location privacy-preserving obfuscation mechanism that does not require collaboration from other users and can provide complete privacy in permissioned blockchain under the presence of PoL.

3 System Overview and Design Goals

In this section, we present the details of the system model and the behavior and attack strategies of the malicious entities in the system. We then formulate the central problem of this chapter and state the goals we set out to achieve in the design of its solution.

3.1 Blockchain System Model

We consider a permissioned blockchain, where its authority also acts as the certificate authority to provide the public and private key pairs to the mobile nodes. The mobile nodes are registered with the system and communicate with each other using the preassigned key pairs. Communication between the nodes takes place using a short-rage communication technology. The nodes can request the authority for new key pairs at any point of time. The blockchain is managed by preassigned mobile edge computing devices (e.g., RSU, Wi-Fi access points, and so on), distributed over a large region. These devices constitute the blockchain nodes and are connected with each other in a P2P network over the Internet. The transactions among the IoT nodes are broadcasted to the blockchain nodes in the blockchain network. The blockchain nodes aggregate and insert the new transactions into the blockchain through a consensus mechanism (e.g., practical byzantine fault tolerance, proof of stake) in a timely fashion (e.g., every 30 minutes). We consider a blockchain architecture similar to the one presented in CreditCoin [11] without considering the rewarding phase. We assume that the mobile nodes have Internet capability to compute the time to reach one location from another with the help of a traffic information provider in real time, e.g., Google Maps. We also assume that the information between the traffic information service provider and a node is anonymous and the provider is independent from the blockchain authority.

3.2 Malicious Entities

In the system, we consider the authority of the blockchain as the malicious entity. It follows the honest-but-curious adversary model in the system. That is, it tries to predict a target node's sensitive spatiotemporal information without violating any protocol of the system or dismantling the way blockchain works. Furthermore, it is not going to hack into the device of a target node. We also consider that, in order to compute the time reachability information, the authority also uses a traffic information service provider. From this point on, we refer to the authority as an attacker. It is important to note that some of the mobile nodes can be malicious. However, as we mentioned earlier in the system model, the mobile nodes can change their public keys at any point of time; the malicious mobile nodes cannot track a target node from their transactions without colluding with the authority. This is a fundamental privacy feature of blockchains. Thus, we focus on the attack strategies of the blockchain authority.

3.3 Attacker's Goal and Strategies

The goal of an attacker is to understand a mobile node's presence at different locations in the temporal domain. In order to do so, it utilizes the time reachability-based spatiotemporal correlation between a node's disclosed locations in the blockchain as its fundamental strategy. Let the random variable O^t_{MU} represent the actual location of a mobile node MU at time t. Given a node's locations l_i, l_j at time t_a, t_b, respectively, the node's probability of being at a location l_h at a discrete time t_q $(t_a < t_q < t_b)$ is

$$Pr^q_{MU}(l_h) = \mathbb{P}\mathrm{r}(O^q_{MU} = l_h | O^a_{MU} = l_i, O^b_{MU} = l_j) \tag{1}$$

The attacker computes $Pr^q_{MU}(l_h)$ using the time reachability correlation as follows:

$$Pr^q_{MU}(l_h) = \begin{cases} 1 & \text{If } l_h \text{ is reachable to and from } l_i \\ & \text{and } l_j \text{ in } (t_b - t_a) \text{ time} \\ 0 & \text{Otherwise} \end{cases} \tag{2}$$

Obviously, it is possible to have multiple locations with $Pr^q_{MU}(l_h) = 1$. Thus, the ultimate goal of the attacker is to minimize the number of such locations, that is,

$$\text{minimize} \left(\sum Pr^q_{MU}(l_h) \right) \tag{3}$$

We also analyze the impact of transaction dropping attacks on location privacy. Note that the scope of this chapter encompasses the analysis of location privacy-invading attacks from a user's point of view, and thus different blockchain-related attacks, such as DDoS, Sybil, 51% attack, and eclipse attack, are not covered here (Fig. 1).

This forms the core of an attacker's strategy. Based on this, we consider mainly the following attacks that can be exploited by the attacker to infer a target node's location information:

- **Collusion with Malicious Mobile Nodes**: Malicious nodes collude with the attacker and provide it with the location information of a target node for profit.
- **Map Matching Attack**: The attacker employs the map information to understand spatially reachable and unreachable location information. A spatially unreachable location refers to a location that cannot be reached at any time using a map service (e.g., the middle of a lake). Thus, $Pr^{\infty}_{MU}(l) = 0$.

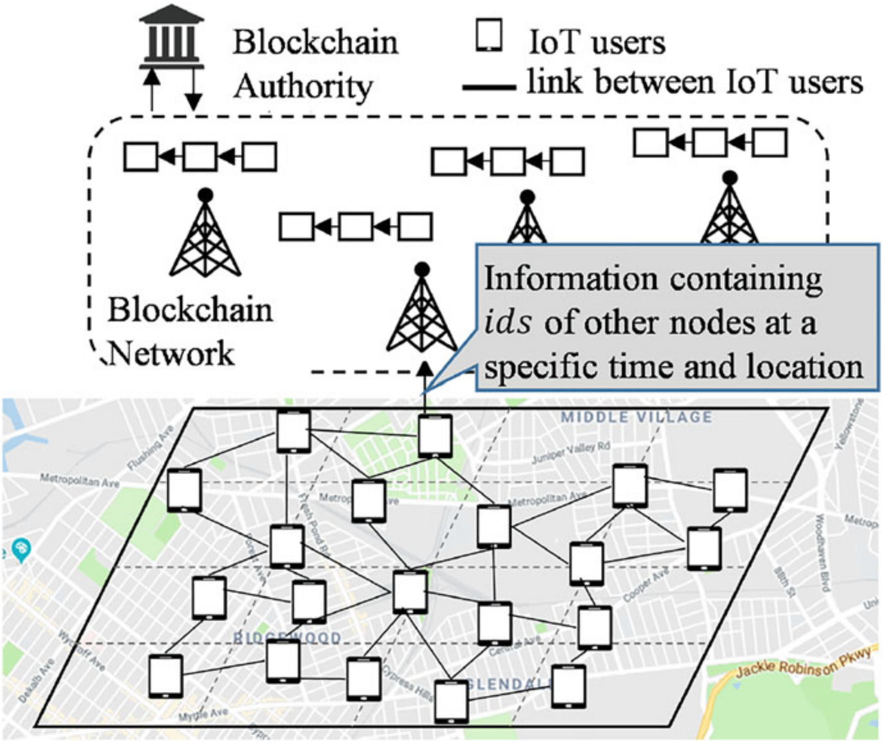


Fig. 1 System model of permissioned blockchain where BC and BA refer to blockchain and blockchain authority, respectively. The BA also acts as certificate authority and trace manager. The mobile IoT nodes are connected with each other in a P2P network using a short-range communication technology. They make transactions with each other and send information on the transactions (e.g., rating about other mobile nodes at a specific location and time) to the nearest blockchain node. Here, each grid refers to a specific location

- **Time Reachability based Path Reconstruction Attack**: In order to reconstruct the actual path between two revealed locations, the attacker can use the time reachability information to construct the valid paths that can be traveled between the two locations within a time limit.

3.4 Problem Formulation and Design Goals

It is clear that there is an important trade-off between location privacy and utilization of the system. The problem lies with the short-range communication technology-based transactions between the mobile nodes that form proof of locations (PoLs) for the nodes. Thus, in order to protect a sensitive location's privacy, a mobile node must remain silent in the network; that is, it must not make any transaction in the network. This leads to the question of how long in both spatial and temporal domains a node must remain silent to protect a sensitive location's privacy. Remaining silent infinitely results in location privacy of 100%, but a system utilization of 0%. In other words, an indefinite silence will incur a 100% *loss of utility*. Hence, the goal of this work is to formulate, design, implement, and evaluate a location privacy-preserving mechanism, called **BlockPriv**, for mobile nodes in the context of permissioned blockchain by solving the following problem:

$$\text{minimize } \{\mathcal{P}^{-1}(l^s), \mathcal{U}(l^s)\} \tag{4}$$

Here, $\mathcal{P}(l^s)$ and $\mathcal{U}(l^s)$ refer to the achieved privacy for sensitive location l^s and the loss of utility due to privacy preservation for l^s, respectively.

To summarize, in the design of the **BlockPriv** mechanism, we intend to achieve the following goals:

- Achieve privacy without collaborating with any other entity in the system.
- Achieve a quantifiable balance between privacy and utility.

4 The BlockPriv Approach

For the sake of clarity and to maintain coherence with the blockchain concept, we first discuss the public key changing technique adapted in **BlockPriv**. In our scheme, we adapt the temporal public key changing concept proposed by Michelin et al. [20]. Here, at a fixed time interval t^{key}, a mobile node will change its public key in order to nullify the possibility of a spatiotemporal linkage attack from malicious nodes. Note that, in our problem, public key changing can only provide privacy to a mobile node against its peers, not against the authority that distributes the keys. Also, this scheme is vulnerable to colluding attacks between the authority and malicious mobile nodes, which is one of the focuses of our work.

At this point, we present the formal definition of location privacy and utility from the perspective of a mobile node. The definition of privacy can be derived from the formulation of the attacker's objective, defined by Eq. 3, as follows:

$$\mathcal{P}(l^s) = \text{maximize}\left(\sum Pr^q_{MU}(l_h)\right) \tag{5}$$

Let us consider a node's last revealed location in the blockchain is l_i at time t_a, and it was at a sensitive location l^s_h at time t_q. It should reveal its location, also known as making a transaction, at an insensitive location l_j at time t_b ($t_a < t_q < t_b$) if and only if

$$\mathcal{P}(l^s_h) = \left(\sum Pr^q_{MU}(l^s_h)\right) \geq \mathcal{N}_h \tag{6}$$

To explain, a node should reveal its location l_j at time t_b in the network to the authority when there exist at least $\mathcal{N}_q$ number of locations, including l^s_h, which are both reachable from and to l_i and l_j in ($\delta t = t_b - t_a$) time. Here, $\mathcal{N}_h$ is a user-defined privacy parameter for location l^s_h. This formulation is applicable only for a single sensitive location. It is also possible that, after l^s_h, the node was also at another sensitive location l^s_p at time t_r ($t_a < t_q < t_r < t_b$) such that, after $\delta t = t_b - t_a$ time, $\mathcal{P}(l^s_h) \geq \mathcal{N}_h$, but $\mathcal{P}(l^s_p)\big) < \mathcal{N}_p$. In such a case, the node should not make any transaction at location l_j at time t_b. Formally, if there are m number of sensitive locations visited by a node between time t_a and t_b, then it will make a transaction with its peers at an insensitive location at time t_b in the network if and only if

$$\mathcal{P}(l^s_i) = \left(\sum Pr^{q_i}_{MU}(l^s_i) \right) \geq \mathcal{N}_i; \quad \forall i = 1, \ldots, m \tag{7}$$

Note that, from t_a to t_b, the node was continuously silent in the network. We call it single or 1 round silence to maintain privacy of the m number of sensitive locations. If a trajectory T_r contains n number of sensitive locations, then the average privacy of each sensitive location in that trajectory is defined as

$$\mathcal{P}(T_r) = \frac{1}{n} \sum_i \mathcal{P}(l^s_i), \quad i = 1, \ldots, n \tag{8}$$

From the formulation of privacy, we can also define the loss of utility due to the application of privacy preservation. Let us consider, at ith round silence, the node opted not to make any transaction at $\mathcal{P}(l^s_h)$ number of locations. In our definitions, this number is the loss of utility of **BlockPriv**. If a node maintained k rounds of silence to preserve privacy of a trajectory T_r with n number of sensitive locations, then the average loss of utility for each sensitive location is

$$\mathcal{U}(T_r) = \frac{1}{n} \sum_{i=1}^{i=k} \mathcal{U}_i \tag{9}$$

This allows us to reconstruct the multi-objective optimization problem, presented in Eq. 4, as a single-objective optimization problem as follows:

$$\begin{aligned} &\text{minimize}\, \mathcal{U}(T_r) \\ s.t. \quad &\mathcal{P}(l^s_i) \geq \mathcal{N}_i; \forall l^s_i \in T_r \end{aligned} \tag{10}$$

Now, we present in detail the mechanism of **BlockPriv** to solve this problem (Fig. 2).

In this mechanism, the mobile nodes are responsible for labeling their sensitive locations and assigning level of privacy to each of them. The nodes utilize radius r to specify the level of privacy for a sensitive location as $\mathcal{N} = \pi r^2$. Let us consider a node MU made a transaction in the network at time t_a at location l_i. Then, it moved

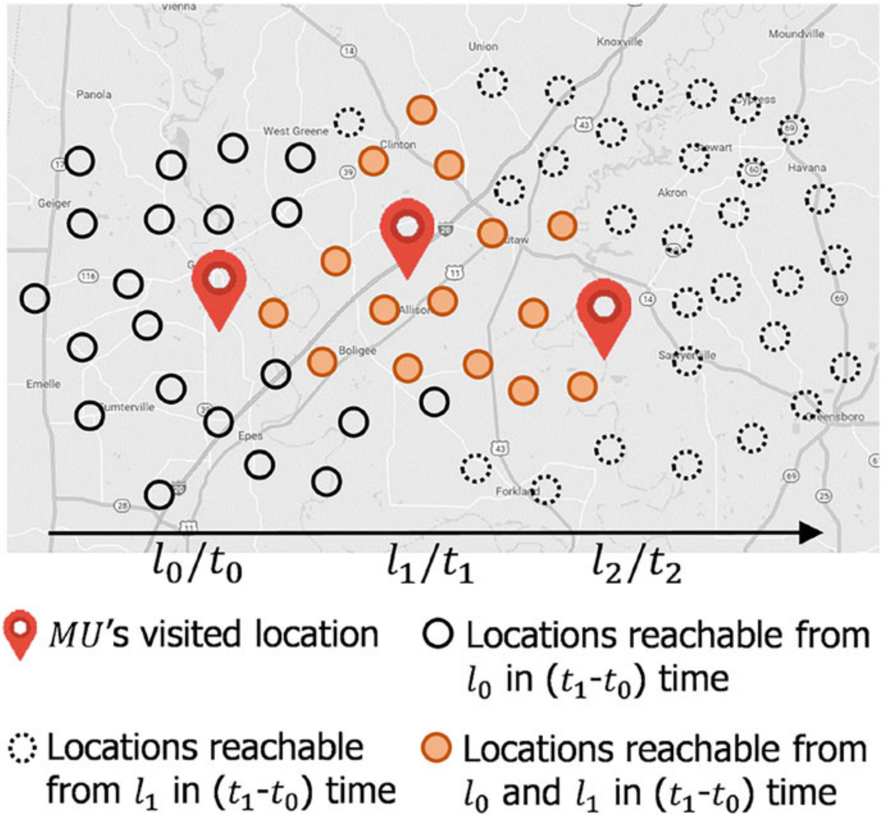


Fig. 2 Illustrated **BlockPriv**: The curve refer to a mobile node (MU)'s actual path between l_0, l_1, and l_2 locations at times t_0, t_1, and t_2, respectively. The location l_1 is privacy-sensitive for the MU. Thus, it remained silent at location l_1. It will make a blockchain transaction at l_2 at time t_2 only when the number of locations reachable from both l_0 and l_2 in $t_2 - t_0$ time meets the privacy requirement for l_1

to a privacy-sensitive location l_h^s at time t_q and did not make any transactions. Then, after every Δt time at location l_j, different from both l_i and l_h^s, it checks the number of locations that are reachable to and from l_i and l_j. Let current time and location be t_b and l_j, respectively. The node first computes the set of all the locations $\mathcal{L}_i$ that are reachable from l_i in $\delta t = t_b - t_a$ time. Next, it computes the set of all the locations $\mathcal{L}_j$ from which location l_j is reachable. Then, $\mathcal{L} = \mathcal{L}_i \cap \mathcal{L}_j$ forms the set of all locations from which both l_i and l_j are reachable in δt time. In other words, each of the location in $\mathcal{L}$ creates a valid 1-hop route from l_i to l_j in δt time. That is, based on the time reachability information, the node can move from l_i to any location $l_l \in \mathcal{L}$ and then move to l_j in δt time. Thus,

$$\mathcal{L} = \{\forall l | (\Phi(l_i, l) + \Phi(l, l_j)) \le \delta t\} \tag{11}$$

Here, $\Phi(a, b)$ refers to the time to get from location a to b. The size of $\mathcal{L}$ defines the privacy level achieved for sensitive location l_h^s in δt time. That is, $\mathcal{P}(l_h^s) = |\mathcal{L}|$. The node will make a transaction at time t_j at location t_b only when $|\mathcal{L}| \geq \mathcal{N}_h$. If there is a total m number of sensitive locations visited by the node in δt time, according to Eq. 7, it will make a transaction at time t_j and location l_b if and only if

$$|\mathcal{L}| \geq \mathcal{N}_i; \quad \forall i = 1, \ldots, m \tag{12}$$

It is understandable that in the case when all the sensitive locations have the same level of privacy, comparing $\mathcal{L}$ with the level of privacy of the latest sensitive location is enough to check whether the condition in Eq. 7 is valid. However, for sensitive locations with different levels of privacy, the MU is required to check whether all the previous sensitive locations' levels of privacy are met before making any transaction.

For a single sensitive location l^s, the maximum loss of utility $\mathcal{U}_{max}(l^s)$ is bounded by the value of its privacy parameter $\mathcal{N}$. The higher the value of $\mathcal{N}$, the higher the $\mathcal{U}_{max}(l^s)$. More specifically, $\mathcal{U}_{max}(l^s) \leq \mathcal{L}$. Certainly, from Eq. 10, we do not want any "extra" loss in utility of the blockchain. Let t_a be the last time a node's location was revealed in the blockchain. After that, at every Δt ($\Delta t \in \mathbb{Z}_{\geq 0}$) time, it computes $\mathcal{L}$ and checks whether it meets the privacy requirement of a set of sensitive locations. That is, after checking $\mathcal{L}$ at time $(t_a + x \times \Delta t)$, it will check $\mathcal{L}$ at time $(t_a + (x + 1) \times \Delta t)$. Here, $x \in \mathbb{Z}_{\geq 0}$. Let t', where $(t_a + x \times \Delta t) < t' < (t_a + (x + 1) \times \Delta t)$, be the time when $\mathcal{L} \simeq \mathcal{N}$. Then, computing $\mathcal{L}$ at $(t_a + (x + 1) \times \Delta t)$ time will certainly impose some extra loss of utilities. Thus, $\mathcal{U}_{max}(l^s) \leq \mathcal{N} + \mathcal{U}'$. Here, $\mathcal{U}'$ refers to the set of insensitive locations at which the MU opted not to make any transaction between time t' and $(t_a + (x + 1) \times \Delta t)$. With the higher value of Δt, the value of $\mathcal{U}'$ will be higher. Thus, Δt should remain as small as possible. However, for resource-constrained mobile nodes, a small Δt means the very frequent computation of the time reachability, which affects the energy of the device. Thus, the compromise between the capability of the device and loss of utility is an issue that needs to be examined: we leave it for our future work. The detail of **BlockPriv** is presented in Algorithm 1.

5 Scheme Analysis

In this section, we present an analysis of the important privacy, utility, and security aspects of **BlockPriv**.

Algorithm 1: BlockPriv

```
Input: Current location $l_{cur}$, current time $t_{cur}$, last revealed location in the blockchain $l_{prev}$
       and time $t_{prev}$, list of sensitive locations $S$, list of level of privacy for the sensitive
       locations $\mathcal{N}$, previous time of key change $t_{prev}^{key}$, key expiration time $t^{key}$
Output: Decision on making transactions.
if $(t_{cur} - t_{prev}^{key}) \geq t^{key}$ then
    Request new key pair from the authority.
    $t_{prev}^{key} = t_{cur}$
if $l_{cur}$ is a sensitive location then
    Append $l_{cur}$ to $S$ and do not make any transaction.
else
    $\delta t \leftarrow t_{cur} - t_{prev}$
    $\mathcal{L}_{prev} \leftarrow$ select all the locations that are reachable from $l_{prev}$ in $\delta t$ time
    $\mathcal{L}_{cur} \leftarrow$ select all the locations from which $l_{cur}$ is reachable in $\delta t$ time
    $\mathcal{L} \leftarrow \mathcal{L}_{prev} \cap \mathcal{L}_{cur}$
    for $(i = 1; i \leq |S|; i++)$ do
        if $|\mathcal{L}| \geq \mathcal{N}(l_i^s \in S)$ then
            Delete $l_i^s$ from $S$
    if $S \neq \emptyset$ then
        Do not make any transactions in the network.
    else
        Free to make transactions.
```

5.1 Privacy Analysis

5.1.1 Privacy Bound

Lemma 1 *If there are multiple numbers of sensitive locations between two revealed insensitive locations, then each of the sensitive locations achieves a privacy level of* $(\max \mathcal{N})$.

Proof Let us suppose that a mobile node MU has visited m number of sensitive locations between l_{prev} and l_{cur} in $\delta t = (t_{cur} - t_{prev})$ time. According to Eq. 12, it will make a transaction at location l_{cur} and time t_{cur} only when all of the sensitive locations' privacy requirements are met. That is, a new transaction will take place only when the length of the set $\mathcal{L} \geq (\max \mathcal{N} = \max\{\mathcal{N}_1, \ldots, \mathcal{N}_m\})$. Thus, even if a sensitive location's privacy requirement is much lower than $(\max \mathcal{N})$, the achieved privacy for ith sensitive location l_i^s in the set is $\mathcal{P}(l_i^s) = |\mathcal{L}| \geq (\max \mathcal{N})$.

5.1.2 Obfuscating Paths

Lemma 2 *If there are any sensitive locations between two revealed insensitive locations l_i and l_j, then, at a minimum, there are* $(\max \mathcal{N})$ *number of* 1*-hop obfuscating paths between the two revealed locations.*

Proof Equation 11 implies that each location in the set $\mathcal{L}$ is reachable to and from l_{priv} and l_{cur} in δt time. Thus, from the point of reachability, each ith location in $\mathcal{L}$ forms a 1-hop path between l_{priv} and l_{cur} in δt time. As a result, each path formed by each sensitive location $l_i^s \in \mathcal{L}$ is obfuscated with $(|\mathcal{L}| - 1)$ number of different other paths in δt time.

5.2 *Utility Analysis*

5.2.1 Loss of Utility Bound

Lemma 3 *If there are multiple numbers of sensitive locations between two revealed insensitive locations, then the maximum loss of utility $\mathcal{U}_{max}(l^s)$ in **BlockPriv** to preserve privacy of a sensitive location l^s is proportional to* $(\max \mathcal{N})$.

Proof Lemma 1 states that whatever the expected level of privacy assigned to a specific sensitive location, the achieved privacy is bounded by the location with the highest level of privacy $\max \mathcal{N}$. Thus, the maximum loss of utility for every sensitive location l^s between the two revealed insensitive locations is

$$\mathcal{U}_{max}(l^s) \leq (\max \mathcal{N}) + \mathcal{U}'$$

5.3 *Security Analysis*

We analyze the efficacy of **BlockPriv** against different location privacy-invading strategies by a malicious authority of the blockchain system. We also briefly discuss the interesting impact of the transaction dropping attack on location privacy.

5.3.1 Collusion Attack

Definition 1 A collusion with malicious mobile nodes is successful if the authority of the blockchain can find a new set of locations $\mathcal{L}*$ about an MU's sensitive location l_i^s such that

$$|\mathcal{L} \cap \mathcal{L} * | < \mathcal{N}_i. \tag{13}$$

Lemma 4 *A combination of time reachability information and collusion with other malicious nodes will not leak the privacy of a target mobile node.*

Proof In **BlockPriv**, a mobile node remains silent in the spatial and temporal domains in order to preserve privacy against an untrusted authority of the blockchain. Thus, even if the authority colludes with some mobile nodes, it will not be able to construct a new set $\mathcal{L}*$ beyond $\mathcal{L}$ that would satisfy Eq. 13. In other words, its understanding of a targeted node's whereabouts will not be made any finer than $\mathcal{L}$ by colluding with other nodes. In fact, collusion with mobile nodes to track a target node is a costly approach. The target node changes its public keys frequently, and to keep tracking it, the authority needs to update the colluding nodes at the same rate. The only way a colluding attack will be successful is if a malicious node physically tracks a target node. However, our work concentrates on providing security against software-based privacy-invading techniques, not on physical observations.

5.3.2 Map Matching Attack

Definition 2 For a sensitive location l^s, a map matching attack is considered to be successful if an attacker can find a set of locations $\mathcal{L}*$ from $\mathcal{L}$ such that

$$(\mathcal{L}* \subset \mathcal{L}*)(|\mathcal{L}*| > 0), \text{ and } Pr^{\infty}_{MU}(l_i) = 0; \forall l_i \in \mathcal{L}* \tag{14}$$

Lemma 5 ***BlockPriv*** *is resilient against map matching attack.*

Proof The mobile node calculates the time reachability information using a real-time map service provider, and thus each location l, selected to form $\mathcal{L}$, is spatially reachable. That is, $\mathcal{L} = \{\forall l \in \mathcal{L} | Pr^{\infty}_{MU}(l) = 1\}$. Thus, $\mathcal{L}* = \emptyset$.

5.3.3 Time Reachability-Based Path Reconstruction Attack

Definition 3 A time reachability-based path reconstruction attack on **BlockPriv** is said to be successful if, for a sensitive location l^s, the authority can find fewer than $\mathcal{N}$ number of paths between two revealed locations for a mobile node.

Lemma 6 ***BlockPriv*** *is resilient against time reachability-based path reconstruction attack.*

Proof According to Eq. 11, every location $l_i \in \mathcal{L}$, including every sensitive location, is reachable from previously revealed location l_{prev} to l_{cur} in δt time. Thus, according to Lemma 2, there are at least max $\mathcal{N}$ number of 1-hop obfuscating paths from l_{prev} to l_{cur} for l_i.

We can now generalize the analysis for multi-hop paths. Let the actual path be $l_{prev} \to l^s_1 \to l^s_2 \to l_{cur}$ and the temporal sequence of this path be $t_{prev} \to t_1 \to t_2 \to t_{cur}$. Hence, $\delta t = \Phi(l_{prev}, l^s_1) + \Phi(l^s_1, l^s_2) + \Phi(l^s_2, l_{cur})$. Assume that, using **BlockPriv**, we got $\mathcal{L}$, where $\{l^s_1, l^s_2\} \in \mathcal{L}$. For the sake of argument, let us consider, for every location $l \in \mathcal{L}'$ ($\mathcal{L}' = \mathcal{L} \setminus \{l_1^s, l_2^s\}$), there exists no multi-hop path. In such a case, if somehow it is known that the node visited multiple locations between l_{prev} and l_{cur}, then the attacker can exclude all the single-hop paths and is able to reconstruct the actual path: $l_{prev} \rightarrow l_1^s \rightarrow l_2^s \rightarrow l_{cur}$. However, in **BlockPriv**, the node remains silent in the network, such that every location in $\mathcal{L}$ exhibits similar probability of being the node's whereabouts under the time reachability condition. Also, such a special case can occur only when $Pr_{MU}^{\infty}(l) = 0; \quad \forall l \in \mathcal{L}'$. This case falls into the category of a map matching attack, and Lemma 5 proves that **BlockPriv** is resilient against such an attack. Hence, time reachability information cannot help a malicious authority to reconstruct the actual path.

5.3.4 Transaction Dropping Attack

In this attack, a mobile node MU_i attempts to drop the transactions between itself and another node MU_j for a specific intention (e.g., preventing the other node from gaining reward out of ill intention or to protect its instance location privacy). There are two cases to consider here. First, MU_j passes the transaction information to the nearest blockchain node, and thus MU_i's location information is revealed. In such a case, MU_i's attempt to protect location privacy will fail. Second, if MU_j's also drop the transaction, then both the nodes' location information will remain undisclosed in the blockchain.

5.3.5 Security Limitations

We are also interested in exploring the following security limitations of **BlockPriv** in the future extension of the work:

(1) *Off-Chain Information-Based Attack.* The attacker can combine off-chain information (e.g., information about the hours of operation of a business) with the map matching attack to devise a better inference model.

(2) *Probabilistic Inference Attack from On-Chain Information.* The attacker can personalize the mobility of the node from the information available on the chain using machine learning algorithms (e.g., Markov chains [34]). Such a model can be exploited to improve the path reconstruction attack.

6 Experimental Evaluation

In this section, we describe the details regarding the experimental evaluation of **BlockPriv**. To properly understand the efficiency and efficacy of our approach, we implemented two cases: locations with (1) similar privacy parameter and (2) different privacy parameters. These two versions will be referred to as **sim-BlockPriv** and **diff-BlockPriv**, respectively.

6.1 Experimental Settings

6.1.1 Dataset Description

In this chapter, we consider the case of making frequent transactions in the network. Hence, we selected Foursquare's New York City (NYC) and Tokyo (TKY) datasets [35] to test the approach with factual data. These datasets contain the check-in information of nodes, in terms of location and time. The number of transactions, locations, location types, and nodes of the datasets are presented in Table 2, and a visualization of the locations in the datasets is depicted in Fig. 3.

6.1.2 Simulation Setup

The datasets do not contain any mark on the privacy-sensitive locations of the mobile nodes. Thus, we mark $\alpha\%$ of the location types as sensitive locations for all the nodes. The different values of the parameters, including the privacy level for a sensitive location r, used in the experiment, are shown in Table 3. For each combination of the parameters, we ran the simulation on both datasets for n number of nodes. As there is a correlation between the number of transactions and the impact of privacy on utility, we selected 100 nodes with the highest number of transactions. We justify this claim by comparing the result with 100 nodes with the least number of transactions. Next, since the datasets do not contain continuous

Table 2 Dataset statistics

Dataset	#Transactions[a]	#Locations	#Types	#Nodes[a]
NYC	227428	38333	400	1083
TKY	573703	61858	385	2293

[a] Originally called "Check-ins" and "Users." In this context, we renamed the variables "Transactions" and "Nodes," respectively

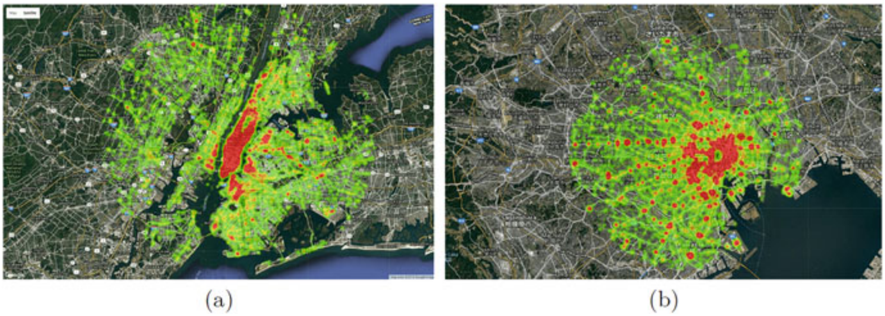


Fig. 3 Locations in (**a**) New York City (NYC) and (**b**) Tokyo (TKY) datasets. Green markers symbolize the locations. The red colors represent the high-density regions

Table 3 Simulation setup parameters

Parameter	Value(s)
r	{500, 1000, 1500, 2000} m
γ	{5,10,15,20}
v	30 miles per hour
α	{2, 4, 6, 8, 10}
n	100

location information, we set a speed (v) for each node to simulate its reachability-based mobility. By nature of mobility, there are cases when a node cannot reach a new location, l_{new}, from a previous location, l_{prev} in a certain time, in the dataset with speed v. In these cases, we continue adding a small value to v (e.g., $v/5$) until it can reach l_{new}. In diff-BlockPriv, the difference in the privacy level for different sensitive locations is set by drawing a random number from the range $\{r - (r \times \gamma\%),\ r + (r \times \gamma\%)\}$.

6.2 Experiment Results

In the experiment, we examine the loss of utility of sim-BlockPriv and diff-BlockPriv. In particular, we examine the following two relationships, fundamental to the design of a privacy-preserving mechanism: (1) loss of utility versus privacy level and (2) loss of utility versus the number of sensitive locations.

6.2.1 Utility Versus Privacy Level

We first examine the relationship between the loss of utility and privacy (in terms of radius r in meters). For example, Fig. 4a–d visually shows this relationship for both sim-BlockPriv and diff-BlockPriv when there are a few number of sensitive locations ($\alpha = 2\%$) and a significant number of sensitive locations ($\alpha = 10\%$). Each data point in a figure refers to the average of the 100 users of a specific city. From these figures, we can make several important occlusions. First, we can draw a clear comparison between sim-BlockPriv and diff-BlockPriv, regarding the impact of privacy level r on the loss of utilities. From the city-level view, for the same value of r, sim-BlockPriv imposes less utility loss than diff-BlockPriv due to the privacy-level randomness associated with diff-BlockPriv. Second, there is an almost linear correlation between the loss of utility and privacy level, regardless of the number of sensitive location types (α) in the dataset. We observe a similar upward trend of loss of utility against the increase in the privacy level for $\alpha = 2\%$ and $\alpha = 10\%$ in both of the datasets. The distribution of loss of utility in Fig. 5 further improves the resolution of this linearity. If we look into the exact numeral values, presented in Table 4, the average Pearson's correlation values [36] are 0.94 and 0.95 for the NYC and TKY datasets, respectively. Such linear correlation and lower loss of utility give

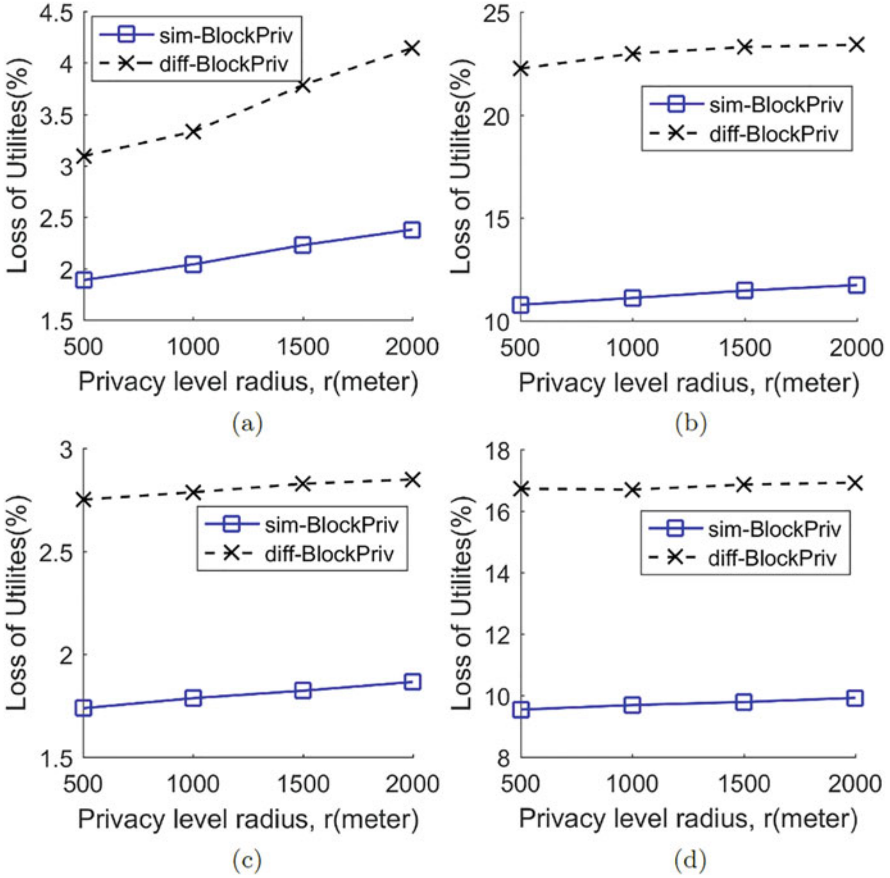


Fig. 4 Average loss of utilities versus privacy level in sim-BlockPriv and diff-BlockPriv. (**a**) NYC ($\alpha = 2\%$). (**b**) NYC ($\alpha = 10\%$). (**c**) TKY ($\alpha = 2\%$). (**d**) TKY ($\alpha = 10\%$)

sim-BlockPriv an upper hand in designing a user-centric privacy scale, which we intend to explore in our extension of this work.

6.2.2 Utility Versus Number of Sensitive Location Types

We then analyze the correlation between loss of utility and the number of sensitive location types (α). While the analysis of the relationship between utility and privacy level shows that the sim-BlockPriv charges less utility loss than diff-BlockPriv, the correlation between utility and the number of sensitive location types further signifies the superiority of sim-BlockPriv. Figure 7a–d presents the average loss of utility for different values of α. We found that, regardless of the value of privacy level r, there is a linear correlation between utility and α. For the same value of r, the

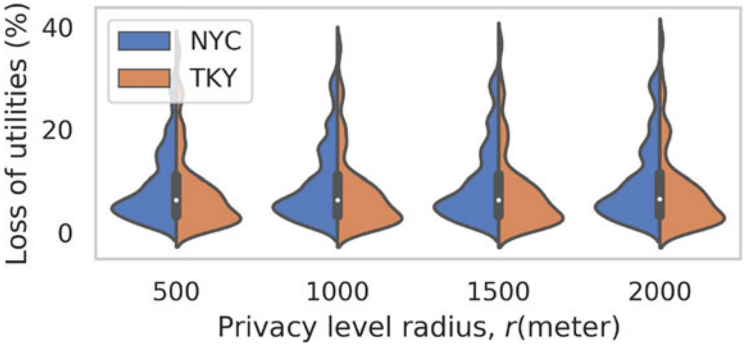


Fig. 5 Distribution of loss of utilities in sim-BlockPriv, regarding different privacy levels

Table 4 Pearson's correlation values

Dataset	Statistics	Loss of utility vs. privacy level	Loss of utility vs. sensitive location types
NYC	Minimum	0.75	0.44
	Average	0.94	0.92
	Maximum	1.00	0.99
TKY	Minimum	0.75	0.74
	Average	0.95	0.95
	Maximum	1.00	0.99

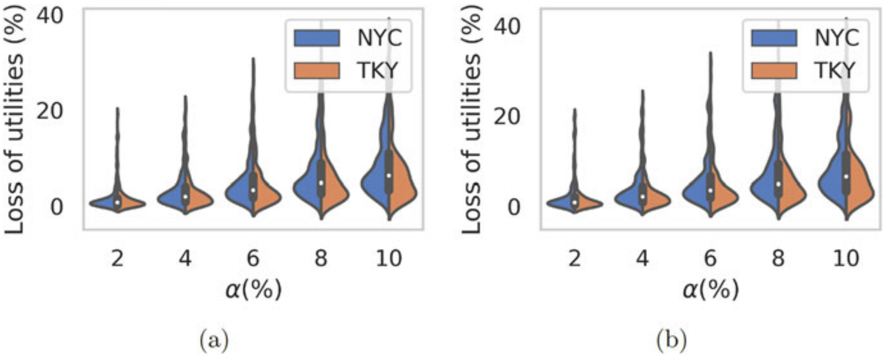


Fig. 6 sim-BlockPriv: comparison of the distribution of loss of utility for different numbers of sensitive location types (α) for $r =$ (**a**) 500 m, and (**b**) 2000 m

higher the value of the α, the higher the loss of utility. However, the increase of loss of utility is slightly sharper in diff-BlockPriv than in sim-BlockPriv. This sharpness is due to the effect of both the increase in the number of sensitive location types and the randomness in the privacy level. As we already know that sim-BlockPriv is better than diff-BlockPriv, we only present the distribution of loss of utility in sim-BlockPriv in Fig. 6. For the same reason, we skipped the depiction of the

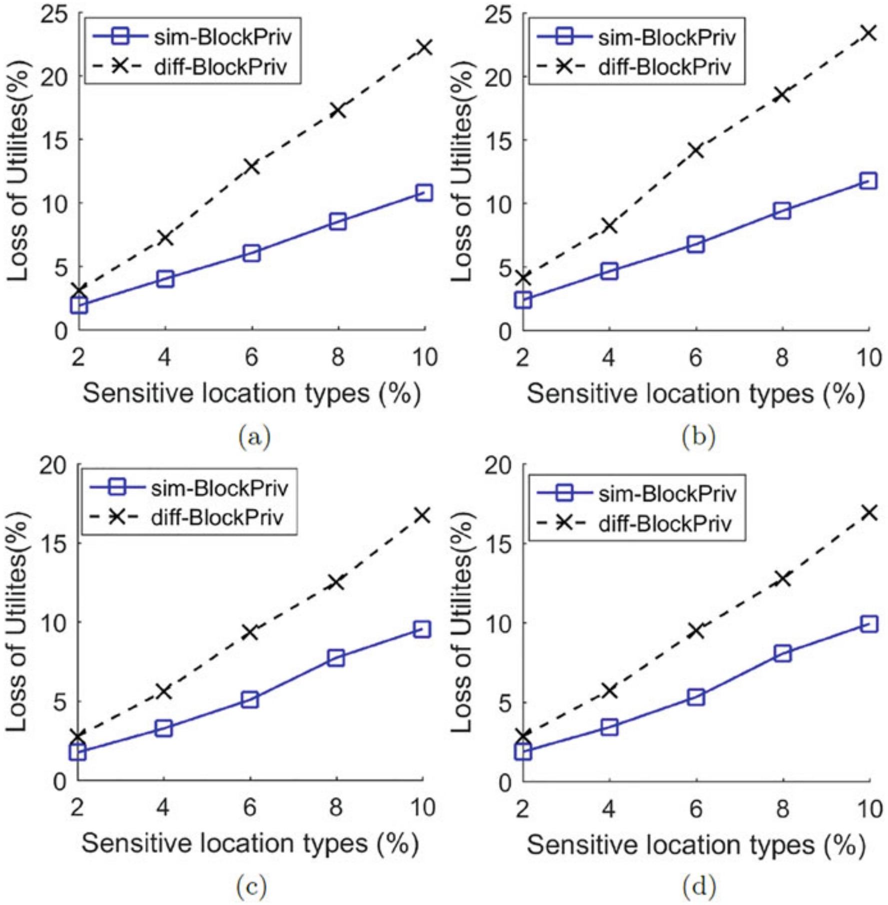


Fig. 7 Average loss of utility versus number of sensitive location types (α) in sim-BlockPriv and diff-BlockPriv. (**a**) NYC ($r = 500$ m). (**b**) NYC ($r = 2000$ m). (**c**) TKY ($r = 500$ m). (**d**) TKY ($r = 2000$ m)

impact of different γ in diff-BlockPriv. Similar to the average values in Fig. 7, the distributions of the loss of utility exhibit a linear correlation. More accurately, the average correlation is 0.92 and 0.95 in the NYC and TKY datasets, respectively. As we mentioned earlier, such a linear correlation can play an important role to make **BlockPriv** usable for privacy-preserving applications.

6.2.3 User-Level Correlation Analysis

Figure 8 depicts the correlation values for loss of utility versus privacy level (U-P) and loss of utility versus the number of sensitive location types (U-S) for 100 users; Table 4 presents different statistics (min, average, and max) on these values. It is

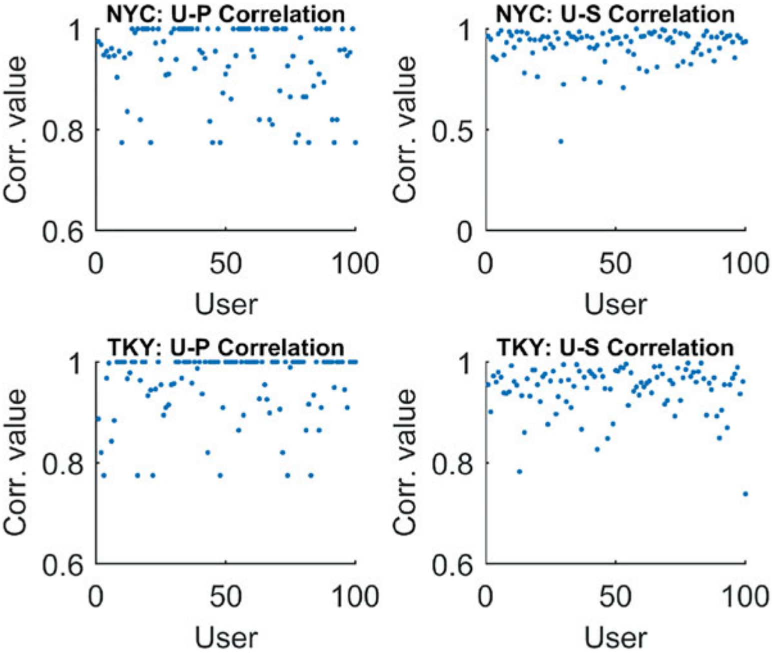


Fig. 8 sim-BlockPriv: correlation values (Corr. value) of loss of utility versus privacy level (U-P) and loss of utility versus the number of sensitive location types (U-S) for 100 users in NYC and TKY datasets

observed that in the NYC dataset, 75% of the nodes have 0.9 correlation for both U-P and U-S. In the case of the TKY dataset, these numbers are 82% and 84%, respectively. Note that these statistics are generated by considering the 100 nodes with the greatest number of transactions in the datasets. We found that, when the number of transactions is fewer, the loss of utility is significantly less. For instance, in both datasets, the 100 nodes with the fewest number of transactions achieved a minimum of 30% less loss of utility than the 100 nodes with the highest number of transactions.

7 Conclusion and Future Direction

In this chapter, we introduce a user-centric obfuscation technique called **BlockPriv**, to preserve location privacy in permissioned blockchain-based IoT systems. As part of this work, we consider that a user cannot falsify its location, and an untrusted authority can correlate locations by considering spatiotemporal constraints to predict unrevealed sensitive locations of a user. We quantify the relationship between the notion of privacy and the utility of the system in **BlockPriv**. We analyze two variations of **BlockPriv**, sim-BlockPriv and diff-BlockPriv, where the first has the same privacy level for all the sensitive locations and the second has a different privacy level for different sensitive locations. We show that there is a linear correlation between loss of utility and privacy level in sim-BlockPriv. Such linearity can be exploited to define a usable privacy scale. In the extended version of this work, we intend to employ a more rigorous model to simulate the mobility of the nodes. Our future work also includes improving the technique by considering different probabilistic attack models based on a combination of off-chain and on-chain information, adapting the approach for the case of continuous transactions in the network, and defining a soft privacy margin to further reduce the loss of utility.

References

1. Z. Wang, F. Xiao, N. Ye, R. Wang, P. Yang, A see-through-wall system for device-free human motion sensing based on battery-free RFID. ACM Trans. Embedded Comput. Syst. **17**(1), 1–21 (2017)
2. S. Bitam, A. Mellouk, S. Zeadally, Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks. IEEE Wirel. Commun. **22**(1), 96–102 (2015)
3. S. Chessa, A. Corradi, L. Foschini, M. Girolami, Empowering mobile crowdsensing through social and ad hoc networking. IEEE Commun. Mag. **54**(7), 108–114 (2016)
4. A.R. Shahid, N. Pissinou, C. Staier, R. Kwan, Sensor-chain: A lightweight scalable blockchain framework for internet of things, in *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (IEEE, Piscataway, 2019), pp. 1154–1161
5. A. Bhattacharjee, S. Badsha, A.R. Shahid, H. Livani, S. Sengupta, Block-phasor: A decentralized blockchain framework to enhance security of synchrophasor, in 2*020 IEEE Kansas Power and Energy Conference (KPEC)* (IEEE, Piscataway, 2020), pp. 1–6
6. A.R. Shahid, N. Pissinou, L. Njilla, S. Alemany, A. Imteaj, K. Makki, E. Aguilar, Quantifying location privacy in permissioned blockchain-based internet of things (IoT), in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (2019), pp. 116–125
7. A.R. Shahid, N. Pissinou, L. Njilla, E. Aguilar, E. Perez, Towards the development of a differentially private lightweight and scalable blockchain for IoT, in *2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW)* (IEEE, Piscataway, 2019), pp. 172–173
8. T. Alam, J. Taylor, J. Taylor, S. Badsha, A.R.B. Shahid, A. Kayes, Leveraging blockchain for spoof-resilient robot networks, in *International Conference on Intelligent Robotics and Applications* (Springer, Berlin, 2020), pp. 207–216
9. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Decentralized Business Review, 21260 (2008)
10. P. Franco, *Understanding Bitcoin: Cryptography, Engineering and Economics* (Wiley, Hoboken, 2014)
11. L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transpor. Syst. **19**(7), 2204–2220 (2018) https://doi.org/10.1109/TITS.2017.2777990
12. M. Amoretti, G. Brambilla, F. Medioli, F. Zanichelli, Blockchain-based proof of location, in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)* (IEEE, Piscataway, 2018), pp. 146–153

13. Z. Yang, K. Yang, L. Lei, K. Zheng, V.C. Leung, Blockchain-based decentralized trust management in vehicular networks. IEEE Int. Things J. **6**, 1495–1505 (2018)
14. A.R. Shahid, L. Jeukeng, W. Zeng, N. Pissinou, S. Iyengar, S. Sahni, M. Varela-Conover, PPVC: Privacy preserving Voronoi cell for location-based services, in *2017 International Conference on Computing, Networking and Communications (ICNC)* (IEEE, Piscataway, 20170), pp. 351–355
15. A.R. Shahid, N. Pissinou, S. Iyengar, K. Makki, Delay-aware privacy-preserving location-based services under spatiotemporal constraints. Int. J. Commun. Syst. **34**(1), e4656 (2021)
16. A.R. Shahid, N. Pissinou, S. Iyengar, J. Miller, Z. Ding, T. Lemus, Klap for real-world protection of location privacy, in *2018 IEEE World Congress on Services (SERVICES)* (IEEE, Piscataway, 2018), pp. 17–18
17. B. Ying, D. Makrakis, Z. Hou, Motivation for protecting selfish vehicles' location privacy in vehicular networks. IEEE Trans. Vehic. Technol. **64**(12), 5631–5641 (2015)
18. J. Bonneau, A. Narayanan, A. Miller, J. Clark, J.A. Kroll, E.W. Felten, Mixcoin: Anonymity for bitcoin with accountable mixes, in *International Conference on Financial Cryptography and Data Security* (Springer, Berlin, 2014), pp. 486–504
19. M.E. Andrés, N.E. Bordenabe, K. Chatzikokolakis, C. Palamidessi, Geo-indistinguishability: Differential privacy for location-based systems, in *Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications security, CCS '13* (ACM, New York, 2013), pp. 901–914. https://doi.org/10.1145/2508859.2516735. http://doi.acm.org/10.1145/2508859.2516735
20. R.A. Michelin, A. Dorri, M. Steger, R.C. Lunardi, S.S. Kanhere, R. Jurdak, A.F. Zorzo, Speedychain: A framework for decoupling data from blockchain for smart cities, in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous '18* (ACM, New York, 2018), pp. 145–154. https://doi.org/10.1145/3286978.3287019. http://doi.acm.org/10.1145/3286978.3287019
21. F. Li, Y. Chen, B. Niu, Y. He, K. Geng, J. Cao, Achieving personalized k-anonymity against long-term observation in location-based services, in *2018 IEEE Global Communications Conference (GLOBECOM)* (IEEE, Piscataway, 2018), pp. 1–6
22. G. Ghinita, M.L. Damiani, C. Silvestri, E. Bertino, Protecting against velocity-based, proximity-based, and external event attacks in location-centric social networks. ACM Trans. Spatial Algor. Syst. **2**(2), 8 (2016)
23. G. Zyskind, O. Nathan, et al., Decentralizing privacy: Using blockchain to protect personal data, in *Security and Privacy Workshops (SPW), 2015 IEEE* (IEEE, Piscataway, 2015), pp. 180–184
24. A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: a distributed solution to automotive security and privacy. IEEE Commun. Mag. **55**(12), 119–125 (2017)
25. M. Singh, S. Kim, Blockchain based intelligent vehicle data sharing framework (2017). Preprint arXiv:1708.09721
26. G. Brambilla, M. Amoretti, F. Zanichelli, Using blockchain for peer-to-peer proof-of-location (2016). Preprint arXiv:1607.00174
27. S. Foley, J.R. Karlsen, T.J. Putniņš, Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Rev. Finan. Stud. **32**(5), 1798–1853 (2019)
28. P. Koshy, D. Koshy, P. McDaniel, An analysis of anonymity in bitcoin using p2p network traffic, in *International Conference on Financial Cryptography and Data Security* (Springer, Berlin, 2014), pp. 469–485
29. A. Biryukov, D. Khovratovich, I. Pustogarov, Deanonymisation of clients in bitcoin p2p network, in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (ACM, New York, 2014), pp. 15–29
30. C. Roulin, A. Dorri, R. Jurdak, S. Kanhere, On the activity privacy of blockchain for IoT (2018). Preprint arXiv:1812.08970
31. R. Sharma, S. Chakraborty, Blockapp: Using blockchain for authentication and privacy preservation in IoV, in *2018 IEEE Globecom Workshops (GC Wkshps)* (IEEE, Piscataway, 2018), pp. 1–6

32. M. Yang, T. Zhu, K. Liang, W. Zhou, R.H. Deng, A blockchain-based location privacy-preserving crowdsensing system. Future Gener. Comput. Syst. **94**, 408–418 (2019)
33. B. Jia, T. Zhou, W. Li, Z. Liu, J. Zhang, A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Sensors **18**(11), 3894 (2018)
34. Z. Montazeri, A. Houmansadr, H. Pishro-Nik, Achieving perfect location privacy in wireless devices using anonymization. IEEE Trans. Inf. Forens. Secur. **12**(11), 2683–2698 (2017) https://doi.org/10.1109/TIFS.2017.2713341
35. D. Yang, D. Zhang, V.W. Zheng, Z. Yu, Modeling user activity preference by leveraging user spatial temporal characteristics in LBSNs. IEEE Trans. Syst. Man Cyber. Syst. **45**(1), 129–142 (2015)
36. J. Benesty, J. Chen, Y. Huang, I. Cohen, Pearson correlation coefficient, in *Noise Reduction in Speech Processing* (Springer, Berlin, 2009), pp. 1–4

A Blockchain-Based Machine Learning Intrusion Detection System for Internet of Things

Jaspreet Kaur and Gagandeep Singh

1 Introduction

In today's era, IoT is the major evolution of Internet also known as Internet of Everything. It creates low-power lossy networks using heterogeneous sensor devices for communicating the information. Some of these sensor devices have resource-constrained features such as limited memory, limited storage, and others have enough memory and resources. Like in the traditional network, these devices and their data also need security such as confidentiality, authenticity, authorization, and availability. But due to the resource constrained nature of some devices, traditional security features are difficult to implement. There are various lightweight security solutions available today such as DTLS, IPSec protocols, Elliptic Curve Digital Signature Algorithm (ECDSA), various types of lightweight intrusion detection/prevention systems (IDSs/IPSs), and many more that are specifically designed for data or payload security. But intruder performs various types of attacks such as DDoS [1] (distributed denial of service), sinkhole attack [1], blackhole attack [1], ransomware attack [2], and many more by just seeing or observing and manipulating the header information. This header information includes both encrypted protocols such as TLS and IPsec and non-encrypted protocols such as HTTP, TCP, IP, UDP (not encrypted in the network due to not to increase latency and less complex operations). Attackers can easily observe this information and manipulate it for their own profit.

There are various approaches in the literature those are focused on these types of attacks, mainly machine and deep learning approaches are considered for predicting or alerting these attacks. Due to resource-constrained nature of IoT devices and for

J. Kaur (✉) · G. Singh
Department of Computer Science and Engineering, Indian Institute of Technology Jodhpur, Jodhpur, India
e-mail: kaur.3@iitj.ac.in

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_6

real-time processing results, some part of these algorithms are implemented at edge of the network and rest processing are done at the cloud.

Recently, blockchain methodology or technique has been taken by industry as well as research community as an innovative or novel technology that create various roles such as managing, controlling, and most valuable securing IoT devices. A blockchain is fundamentally a decentralized, distributed, shared, and immutable database ledger that stores any type of data and transactions across a peer-to-peer (P2P) network [1]. Due to various advantages of this technology, it has various use cases such as cryptocurrency, decentralized apps, securing machine learning algorithms, Internet of Things as smart city, smart health care, and many more. But in this chapter, we mainly focus on how combinations of blockchain, machine or deep learning algorithms, and edge computing are to be used for security of IoT devices through seeing the header part of the packets.

The rest of the chapter is organized as follows: Sect. 2 discusses various IoT security attacks and their existing solutions. Potential combination of blockchain features with respect to IoT has been discussed in Sect. 3. In the next section, we have been surveyed some recent related work in the direction of ML and DL methods for the IoT security. In Sect. 5, we mention some possibilities of combining these three technologies (blockchain, IoT, and ML/DL methods) as well as our proposed work in this direction for the security of IoT data. Experimentation and result analysis have been given in Sect. 6. Finally, we conclude our work with some future directions.

2 IoT Security Attacks and Their Solutions

Intruders perform various attacks to disturb the functionality of IoT networks. These attacks are occurred due to the weaknesses or absence of security features such as authentication, authorization, and many more. Some of these security issues and their implications along with their existing solutions in the literature are presented in Table 1. These attacks and their security measures are to be taken either at data part or at header part features of the network packets. There are various technologies such as cloud computing, edge or fog computing, blockchain, SDN (software-defined networking), lightweight cryptographic algorithms, machine/deep learning techniques, etc. that are to be used in the literature for providing security to IoT devices/network. But in this chapter, our main focus is on how we can combine blockchain, ML and DL algorithms, and edge computing for IoT data security.

3 Blockchain of Things (Blockchain with IoT)

Nowadays, blockchain technology is used almost everywhere due to their fundamental features such as a decentralization of nodes, distributed, shared, and

Table 1 Summary of IoT security threats, implications, and their existing solutions

Security issues	Implications	Proposed solutions
Sybil and Spoofing Attacks [1, 3–8]	Network disruption, Denial of Service (DoS)	Signal Strength Measurements, Channel Estimation, Random Traversing of Social Graphs and IDS
RPL Routing Attacks [1, 5, 9–12]	Eavesdropping, Man-in-the-Middle Attacks, Rank and Version number attacks	Hashing and Signature based Authentication and Observing Node Behavior
Sinkhole, Blackhole Attack and Wormhole Attacks [1, 3–5, 8, 13–15]	Denial of Service, Disrupt the network topology	Rank Verification Through Hash Chain Function, Trust Level Management, IDS (Intrusion Detection System)
Authentication and Secure Communication related Attacks [1, 3–5, 16, 17]	Privacy and Integrity Violation	Compressed AH and ESP, Header Compression and Software Mode AES,IACAC using the Elliptic Curve Cryptography, Hybrid Authentication, Distributed Logs and Homomorphic Encryption
Transport Level End-to-End Security Attacks [1, 3–5, 18, 19]	Privacy Violation	DTLS-PSK with Nonces, 6LBR with ECC, Compressed IPSEC, DTLS Header Compression,IKEv2 using Compressed UDP and AES/CCM based Security to Identification and Authorization
Insecure Software/Firmware Attacks [1, 3–5, 20]	Privacy Violation, Denial of Service, Network Disruption	Regular Secure Updates of Firmware, Use of File Signatures, and Encryption with Validation
Middleware Security Attacks [1, 3–5, 21]	Privacy Violation, Denial of Service, Network Disruption	Secure Communication using Authentication, Security Policies, Key Management between Devices, M2M Security
CoAP Security Attacks [1, 3–5, 22–24]	Network Bottleneck, Denial of Service	Mirror Proxy, TLS/DTLS & HTTP/CoAP Mapping, TLS-DTLS Tunnel, Message Filtration by 6LBR

immutable database ledger that stores any type of data and transactions across a peer-to-peer (P2P) network. It maintains as a link list blocks of data that have been time-stamped and verified by miners. The blockchain provides data authentication and integrity using strong cryptographic algorithms such as elliptic curve cryptography (ECC) and SHA-256 hash method. Basically, the block data contains a list of all transactions or assets along with a hash to the previous block for maintaining a linked list. So that it can track a history events of the assets and gives an interoperable overall distributed trust. In blockchain, each transaction is validated by a majority agreement of miner nodes those are actively involved in validating and verifying transactions [1, 25, 26]. Due to these advantages of this technology, it can be used for IoT devices as well.

3.1 Advantages of Blockchain of Things

Below we have mentioned some of the advantages of blockchain of things:

1. **Address Space and Identity:** IPv6 protocol is unable to cooperate to these resource-constrained network (IoT network). But using blockchain, it eliminates IANA (centralized authority). In addition, blockchain provides 160-bit unique address space for the identification of IoT devices, which is more than IPv6 128-bit address space, and this makes blockchain a more scalable solution for IoT than IPv6. It also provides a set of various features and relationships that are to be stored on the blockchain.
2. **Decentralized and Trust:** Blockchain eliminates centralized server and maintains a peer-to-peer network that builds trust between parties and IoT devices. Due to its decentralized behavior, it reduces transactional cost and accelerates transaction speed.
3. **Integrity and Pseudo-anonymity:** All transactions made to or by an IoT device are cryptographically proofed, signed by the true sender, and verified by majority nodes. All these messages are stored on the blockchain ledger and can be tracked securely, which provide integrity and authentication of transmitted data. Blockchain uses public key as user address which provide pseudo-anonymity.
4. **Authentication, Privacy, and Authorization:** Blockchain smart contract provides a decentralized single and multiparty authentication rules, authorization access rules, and data privacy access rules of less complexity when compared with traditional Internet Protocols. These smart contracts can create the various logics of code for protecting the IoT devices.
5. **Security in Transmission:** Basic IoT connection protocols such as HTTP, MQTT, CoAP, RPL, and 6LoWPAN are not secure by design. There are several security protocols such as DTLS, TLS, and IPSec that are used to provide secure communication in IoT. But these security protocols require high computation and memory requirements and used centralized PKI protocol for key management and distributions. With blockchain, centralized PKI protocol is totally mitigated, as each IoT device would have its own unique id and asymmetric key pair. This provides us lightweight or simplify solution that would satisfy the requirements of resource-constrained IoT devices.

3.2 Disadvantages of Blockchain of Things

Despite various advantages of blockchain platform, it also has some limitations when this technology is applied on the IoT devices such as:

1. Resource-constrained nature of some IoT nodes incapable of storing large blockchain database, which leads to the **scalability** issues.

2. **Computationally intensive task** as mining not to be done at all IoT devices due to memory and CPU power restrictions.
3. In some use cases, **transparency** of the confidential data is harmful to the users.
4. Blockchain itself is a **naive protocol** (has inbuilt limitations).

3.3 Some Related Work of Blockchain of Things

Researchers and industrialist used various approaches for combining these two technologies for taking the advantage of both and reducing the above limitations as much as possible. Today, blockchain can be applied at almost all of the applications of IoT such as smart city, smart healthcare, smart vehicle, smart grid, crowd-sensing applications, and many more. The general architecture of blockchain of things has been shown in Fig. 1. Various blockchain platforms and some of the recent related work that support blockchain with IoT are given as follows:

Bitcoin [27, 28] is the first blockchain cryptocurrency platform for IoT domain which provides micro-payments to the autonomous IoT devices. It can be a drawback since decreasing the value of the coin can negatively affect the performance of application. So, there is another blockchain platform named as Ethereum [28, 29] by which decentralized application era has begun. It uses the concept of smart contract for securing logics, policies, and permissions that react after a specific

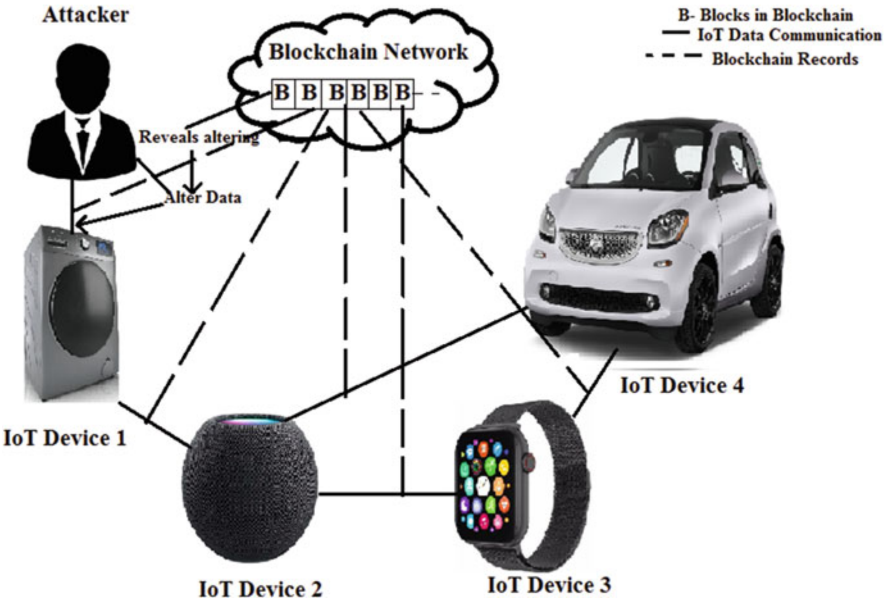


Fig. 1 General architecture of blockchain of things

event. As in paper [30, 31], the authors developed a leave application management system using Blockchain Smart Contract managed by heterogeneous IoT devices at Ethereum platform. Hyperledger [28, 32] is an open-source platform or framework for permissioned blockchain applications. It provides various factors for agreement and membership. Distributed applications can be made by this platform using general purpose languages. IoT devices can provide data to the blockchain via the IBM Watson IoT Platform, which use for managing devices and allows data analysis and filtering. IBM's Bluemix platform provides this integrated utility as blockchain as a service. The use of this framework speeds up application prototyping.

The Multichain [33] platform provides a new framework for the development and deployment of private blockchains. Multichain uses an application that enhances the core functionality of the original Bitcoin API and allows the management of permissions, transactions, portfolios, assets, etc. It is also a useful platform for deploying blockchain of things. In paper [34], the authors use the multichain platform to IoT devices for evaluating the use of cloud and fog as hosting platforms of blockchain.

One another platform known as IOTA [35] uses DAG (Directed Acyclic Graph) data structure, blockless framework for more scalable solution to blockchain of things. But this platform is on their naive state means we do not know how much it will lead to be scalable and reliable in future.

In paper [36], they use edge cloud method for solving the scalability and security issues for blockchain of things. They write smart contacts as for analyzing the behavior of IoT devices and resource allocation at edge devices for resource-constrained nodes and finally mitigate the malicious users for setting the flag in the smart contract. In paper [37], the authors introduce blockchain in Internet of Things using smart home environment at which they use local blockchain for policy checking purpose whether the devices are authorized or not and also use cloud structure for storation of data. They also use the concept of overlay networks for securing the data at cloud and easy management of the different network environments.

In paper [38], iExec corporation introduces a new method such as blockchain-based decentralized cloud computing at which they give a web interface using Ethereum platform to IoT devices for communicating with blockchain. These blockchain services are managed at the decentralized cloud using off-chain computation and rules managed via scheduler. In paper [39], the authors talk about Blockchain of Things by establishing an analytical model for considering spatiotemporal domain to maximizing transaction throughput, maximizing performance analysis, and finding the optimal node deployment location. In paper [2, 12], the authors use blockchain for RPL and ransomware attacks.

In summary, all the works related to blockchain of things are considered one or multiple of these as usage of:

1. Decentralized Cloud
2. Use of Distributed Edge Computing or Database
3. Use of Off-Chain Data

4. Deletion of Data Blocks (Depending on Use Case)
5. Use of Multichain
6. Use of Different Structure as IOTA
7. Use of Less Computation Consensus Algorithm
8. Use of Light Weighted Software as Ethereum lite

These above approaches are provided for solving the limitations of both IoT and blockchain technology or combining these technologies more easy and advantageous way.

4 ML and DL Algorithms in IoT Security

For securing any IoT device from various attacks, there is a probability to proactively predict these attacks using various machine learning and advanced deep learning techniques.

In the literature survey [3, 4], we have seen that there are various works to be done into this direction. They use various approaches for detecting and predicting the IoT attacks such as malware attacks, routing attacks, impersonation attacks, and many more at every layer of IoT framework such as perception layer, network layer, and application layer. The general architecture of ML/DL algorithms in IoT data security has been shown in Fig. 2. In this general architecture, the researchers must create their dataset with normal as well as attack packets via various IoT devices such as smart phone, smart watch, smart car, etc. and then apply various ML as well as DL methods for attack detection. The ML and DL algorithms used in this process are:

1. DT (Decision Tree), SVM (Support Vector Machine), KNN (K-Nearest Neighbor), Naive Bayesian, CNN(Convolution Neural Network), RNN (Recurrent Neural Network) in supervised algorithms
2. K-Mean Clustering, PCA (Principal Component Analysis), AE (Auto Encoder), RBM(Restricted Boltzmann Machine), DBN (Deep Belief Network) in unsupervised algorithms
3. Some hybrid methodologies or semisupervised methods such as GAN (Generative Adversarial Networks) and many more
4. RL (Reinforcement Learning)

In paper [6], the authors use three DDoS (distributed denial of service) attacks such as TCP SYN flood, a UDP flood, and a HTTP GET flood for performing attack on IoT devices. They use Mirai-infected devices for performing attack and use various features such as Packet Size, Inter-packet Interval, Bandwidth, and many more in various ML algorithms and neural network methods for prediction analysis of attacks. Similarly in paper [8], the author uses various ML techniques for detecting various preliminary attacks and compares those results to available IDS (Intrusion Detection System). In paper [40], the author proposes a semisupervised methodology for detecting these nodes attack. There are several intrusion detection

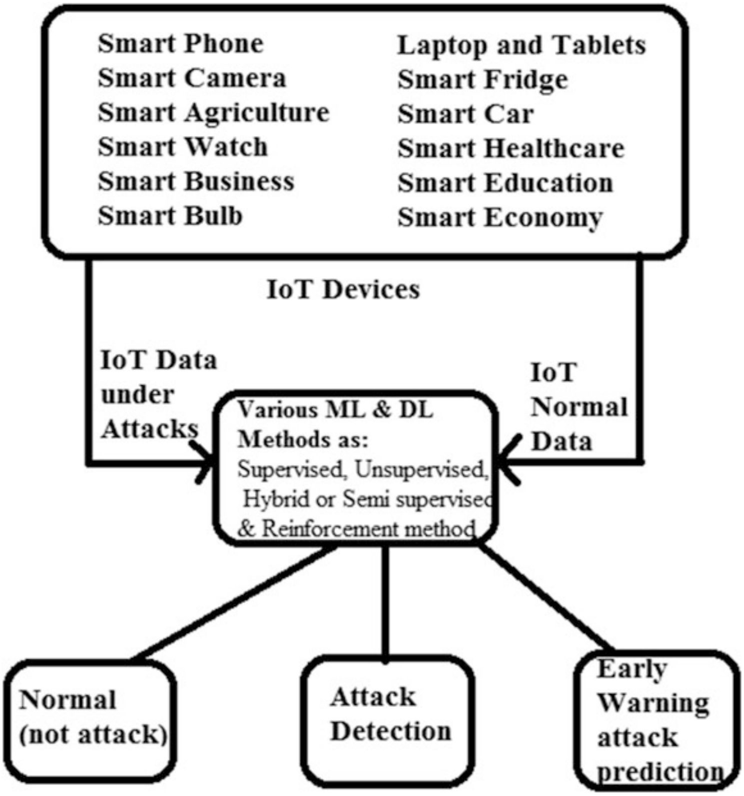


Fig. 2 General Architecture of ML and DL algorithms in IoT Security

systems (IDSs) that are to be proposed into this direction such as modified SNORT [41], SVELTE [5], RPiDS [42], and many more.

There are various technologies such as cloud computing and edge or fog computing along with training data distribution or model trainer distribution that are to be used for lightweight implementation of ML and DL algorithms in resource-constrained IoT devices. Despite that, still we have various open challenges into these directions as follows:

1. Less availability of security related IoT datasets
2. Learning from low-quality data to securing IoT devices
3. IoT data augmentation and fusion
4. How to apply ML and DL algorithms for IoT security in interdependent and interactive environments
5. Security and privacy of ML and DL algorithms and their data
6. Possible misuse of ML and DL algorithms by attackers and corrupted ML and DL algorithms

7. Integrating DL/ML algorithms with other technologies such as blockchain, cloud computing, and edge computing for IoT Security

5 Combining Technologies (Blockchain, IoT, and ML/DL) for IoT Security

There are various suggestions given in the literature [1, 3] or article [43] regarding the combinations of these technologies for IoT devices and data security. All these methods have started with heterogeneous IoT device data collection. They have used different technologies such as blockchain, edge computing, cloud computing, and various ML and DL techniques for pattern analysis as well as security purposes. There are already various examples or solutions such as supply management system, smart infrastructure, and many more that have used combination of these technologies. The combination of these maintains security of IoT data and devices, security of ML/DL input data and algorithms, as well as maintaining data analysis/quality. Figure 3 can also illustrate these technology combinations. Despite these valuable suggestions, as per our knowledge, we have not found any simulation or real-time implementation that combined all of these technologies for packet header security. There is a vast opportunity in this direction to work. So, our work is also a small contribution in this area, which leads this research a step ahead.

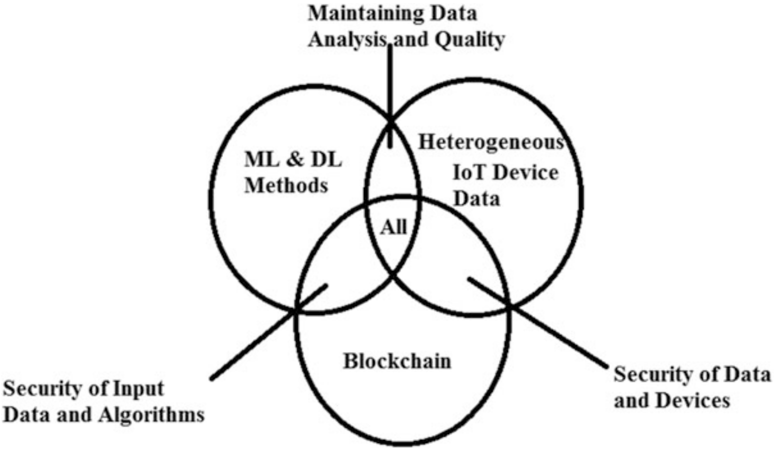

Maintaining Data Analysis and Quality
ML & DL Methods
Heterogeneous IoT Device Data
All
Blockchain
Security of Input Data and Algorithms
Security of Data and Devices

Fig. 3 General Framework of Combination of these Technologies (Blockchain, IoT, ML and DL methods)

5.1 Brief Summary of Our Problem Statement

Various machine learning and deep learning approaches are valuable for header-based prediction IoT security attacks and provide more accurate results unless and until the training data or prediction data is not manipulated by the attacker, until algorithms of machine learning process are not hacked by intruder and quality of the heterogeneous devices data are accurate means data fusion has been done appropriately as well as need appropriate data handling in edge/cloud storage. These above limitations motivate us to develop a new platform which mitigates some of the above issues as low as possible. Our new platform combines blockchain, ML/DL algorithms, and edge storage for handling heterogeneous IoT devices data security.

5.2 Our Proposed Approach

In our approach, we have combined the blockchain, ML/DL methods, and edge storage for providing the header-based security attack detection (IDS) in heterogeneous IoT environment. Briefly, our methodology works as follows:

In a heterogeneous IoT environment, there exist some low power/memory devices as well as some high computing devices. In this IoT environment, there are various attacks possible such as spoofing attacks, ransomware attack, DDoS attacks, and many more. Here, we deal how to detect these attacks with secure ML-based IDS by just seeing the header information. Here, we have applied the blockchain technology for securing the communicating data and code logic of ML/DL algorithms along with the proper embedding of it at various heterogeneous IoT devices. It means that there are some low-powered or low-resource IoT devices that directly interact with the blockchain running at the edge node devices (high-power IoT devices). These node devices are treated as thin client Ethereum node (not performing mining process and storation of blockchain at them, but key generation is performed on these nodes itself) and all the data sent by them to the edge nodes are authenticated by digital signature (access control in private blockchain) and provide integrity feature using private blockchain.

A private blockchain is managed by the edge nodes devices. These edge devices are the high-power IoT devices that perform mining process of blockchain and storation of blocks. These devices also use a load balancer method for incoming packets transactions. A smart contract written on private Ethereum separates the data and header part of packets, and finally header part of the packets are saved in the blockchain. This discussed procedure maintains integrity of training data.

After that at the edge node devices, we use some machine or deep learning algorithms at blocks of data (header information) for prediction of attacks vs normal data. These ML and DL algorithms are also secured by smart contracts. Based on the use case or availability of resources, we take data from blockchain for predicting attack based on some time frame. Due to the resource limitation, after particular

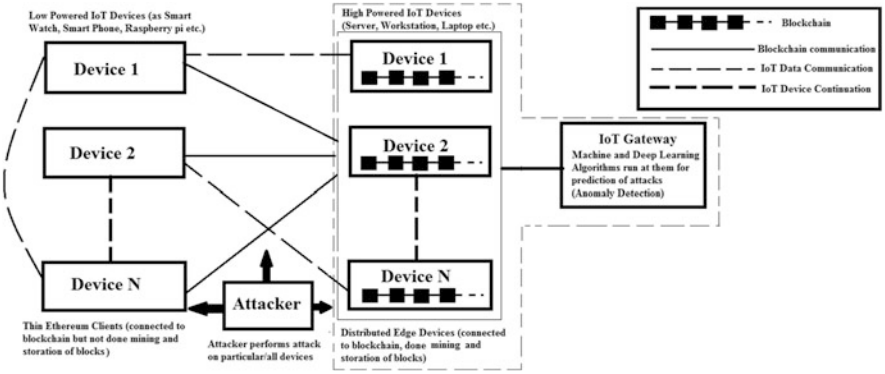

Low Powered IoT Devices (as Smart Watch, Smart Phone, Raspberry pi etc.)
High Powered IoT Devices (Server, Workstation, Laptop etc.)
Device 1
Device 2
Device N
Device 1
Device 2
Device N
Attacker
Blockchain
Blockchain communication
IoT Data Communication
IoT Device Continuation
IoT Gateway
Machine and Deep Learning Algorithms run at them for prediction of attacks (Anomaly Detection)
Thin Ethereum Clients (connected to blockchain but not done mining and storation of blocks)
Attacker performs attack on particular/all devices
Distributed Edge Devices (connected to blockchain, done mining and storation of blocks)

Fig. 4 Overview of our proposed framework

time limit, some older blocks of data are to be vanished or no use at all. Quality of heterogeneous devices data (data fusion) are also managed by ML or DL and feature extraction techniques (what header features are to be taken for predicting the attack).

We need a large amount of data for high accuracy prediction. But ML algorithms are less complex to implement than DL algorithms. So, we use 2 methods to handling the complexity of algorithms as follows: for ML algorithms (less complex) like decision tree, K-means, we take training data distribution method to divide the data at various edge nodes, and then ML algorithm is applied on these data and final results are aggregated at the gateway node. But in the DL learning methods (high complex) such as convolution neural network (CNN) and recurrent neural network (RNN), we take model trainer distribution method at which DL algorithm's independent modules are given to the edge nodes and training data is passed to one edge node, after that second one, and so on until the last one (pipe lining of the data). Finally, the result has to be passed to the gateway. The below is our complete proposed framework, shown in Fig. 4. Our experiment simulation to this framework has little difference due to the limitation in the simulation environment. But it can be completely extended to the real-world scenario as discussed above. Our proposed framework is generalized, which means it is applicable to any domain (smart home/University/Airport etc.) and can detect all types of intrusions/attacks (DDoS/ransomware, etc.) in heterogeneous IoT environment by ML-based intrusion detection system (by packets header portion only). Take an example of a smart home scenario in this framework; if an attacker performs some attack such as DDoS attack, ransomware attack at that home, then it can be easily detectable by gateway node. We can also detect these attacks at a particular locality/community of smart homes by some extension of our proposed work. Then, our proposed framework is applied to each smart home, and then each smart home gateways in that is connected to peer-to-peer network, which means they maintain a separate blockchain for deciding attack at that locality level. So, that we can detect the major localities or areas at which these attacks are frequently happened. Once the attack is detected, then that attack is easily mitigated by removing that attacker node by sending disassociation or deauthentication packets and set the flag bit in smart contract so that further intruder packets are not treated via blockchain (for saving computational and memory resources).

6 Experimentation and Results

There are various attacks occurred as mentioned above due to the header part of packets in IoT devices, and our proposed approach is generalized, which means it can detect any kind of attacks. But in this chapter, we simulate only DoS/DDoS attack protection via our proposed approach taking assumption only for the single smart home environment. This simulation has been done at single computer system (8 GB RAM and I7 core processor).

We used Remix IDE [28, 44], a well-known platform for development and testing of blockchain utilities, for experimentation purposes of the smart contract. A smart contract is developed for the separation of data and header part of packets along with maintaining the access control of IoT devices. ML and DL algorithms integrity will be maintained by us in the extended/future work. In this platform, we used 5 IoT device accounts for simulation and to collect dataset (attack and non-attack packets). The deployment of the smart contract resulted in a transaction cost of 975040 gas and an execution cost of 707364 gas. Initially, we take 3 types of headers such as TCP, UDP, and ICMP for performing the DoS/DDoS attack (Low Orbit Ion Cannon (LOIC) application [45] for TCP and UDP flood and PING utility for ICMP flood). For separation of header and data packets for these three protocols, the transaction cost and execution costs of the smart contract are given in Table 2. For learning methodology (in Fig. 5), we trained a sequence model [46] for predicting DoS/DDoS attacks on TCP, UDP, and ICMP packets. The model architecture consisted of three layers: the first one being LSTM [47] with return state=True, the second layer was dropout to avoid overfitting during training, and the last layer was dense layer with sigmoid activation, which returned a number between 0 and 1, signifying the probability of DDoS attack on the input sequence of packets. The shape of the input to the LSTM was, f × p, where f denotes the number of packets being fed to the LSTM as a sequence and p denotes the length of the feature of vector of the packet. We collected these features of header for attack detection as time stamp of the packet, source and destination in IP layer of the packet, source and destination of Ethernet packet, length of the packets in bytes, source and destination ports, ICMP sequence number, and some others fields. We trained our model on around 10,000 sequences of packets (50% being DoS/DDoS and rest non-DoS/DDoS) with a validation split of 0.2 and a batch size of 32, optimizer was Adadelta, loss function was binary cross entropy, and binary accuracy was used as metric. The training labels were 0 for non-DDoS packets and 1 for DDoS packets. When we implement our proposed method using these parameters, then the outcome results are quite satisfactory as shown in Table 3. We can also say that by seeing these results, our proposed approach accuracy and efficiency remain as high as now when we implement this at real-time dataset or increase our simulation dataset.

Table 2 Costs of smart contract for header and data separation

Protocol used	Transaction cost	Execution costs
TCP (Transmission Control Protocol)	205759 gas	173607 gas
UDP (User Datagram Protocol)	66529 gas	63225 gas
ICMP (Internet Control Message Protocol)	264698 gas	228194 gas

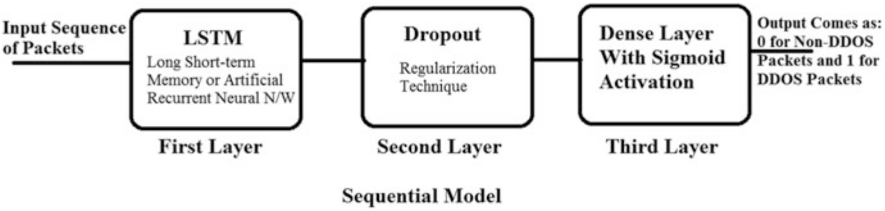

Input Sequence of Packets
LSTM
Long Short-term Memory or Artificial Recurrent Neural N/W
First Layer
Dropout
Regularization Technique
Second Layer
Dense Layer With Sigmoid Activation
Third Layer
Output Comes as: 0 for Non-DDOS Packets and 1 for DDOS Packets
Sequential Model

Fig. 5 Data learning methodology as sequence model

Table 3 Accuracy and F1-Score Results for DoS/DDoS Attacks

Protocol used	f value	p value	Threshold	No. of epochs	Binary accuracy	F1-Score
TCP	4	24	0.7	10	81.55	0.95
UDP	12	24	0.7	10	85.79	0.88
ICMP	16	24	0.7	10	86.28	0.84

7 Conclusions and Future Directions

Today, increased usage of IoT devices makes them very prone to attacks. There are various lightweight cryptographic approaches that are to be used in data protection of these devices. But still these attacks are to be occurred due to manipulating or observing the header part of the packets (encrypted and non-encrypted both). There are various methods to be used for protecting these attacks, specifically ML and DL methods. But these learning methods' accuracy totally depends on the security of training data and on the integrity of learning algorithms. So, we develop a new model that removes above limitations as low as possible using a combination of new technologies such as IoT devices along with Blockchain, ML or DL methods, and edge or fog computing. Our proposed framework is very useful due to the ML and DL calculations occurred at the edge distributed computing that reduce processing time compared to the cloud computing and also use blockchain smart contract for both providing security to input data and access control to the IoT devices. For the implementing scenario, we simulate a single smart home environment with 5 IoT devices in Ethereum blockchain and detect DoS/DDoS attacks those are occurred via TCP, UDP, and ICMP packet headers via the LSTM method. From the produced results, we say that our proposed model is working quite satisfactory.

Some extension or more detailed implementation (observations) will have to be done in future work for improving the efficiency of our proposed work as follows:

1. We firstly take real-time environment to implement our model on the single/multiple smart homes or on another smart infrastructure or environment.
2. We will also implement or detect various IoT device attacks such as ransomware attack, sinkhole attack, or blackhole attack.
3. We will use various lightweight ML and DL algorithms for improving result accuracy and quality of data.
4. We will use software-based load balancing techniques for incoming transactions at edge IoT devices.
5. We will apply blockchain smart contract at ML/DL algorithms (code) itself.

References

1. M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018)
2. J. Kaur, A Secure and Smart Framework for Preventing Ransomware Attack. arXiv preprint arXiv:2001.07179 (2020)
3. M.A. Al-Garadi, et al., A survey of machine and deep learning methods for Internet of Things (IoT) security. arXiv preprint arXiv:1807.11023 (2018)
4. F. Restuccia, S. D'Oro, T. Melodia, Securing the Internet of Things in the age of machine learning and software-defined networking. IEEE Internet Things J. **5**(6), 4829–4842 (2018)
5. S. Raza, L. Wallgren, T. Voigt, SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Netw. **11**(8), 2661–2674 (2013)
6. R. Doshi, N. Apthorpe, N. Feamster, Machine learning DDoS detection for consumer Internet of Things devices, in *IEEE Security and Privacy Workshops (SPW)* (IEEE, New York, 2018)
7. J. Kaur, MAC layer management frame denial of service attacks, in *International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)* (IEEE, New York, 2016)
8. J. Kaur, Wired LAN and Wireless LAN attack detection using signature based and machine learning tools, in *Networking Communication and Data Knowledge Engineering* (Springer, Singapore, 2018), pp. 15–24
9. A. Dvir, L. Buttyan, VeRA-version number and rank authentication in RPL, in *IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems* (IEEE, New York, 2011)
10. H. Perrey, et al., TRAIL: Topology authentication in RPL. arXiv preprint arXiv:1312.0984 (2013)

11. D. Airehrour, J.A. Gutierrez, S.K. Ray, SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Futur. Gener. Comput. Syst. **93**, 860–876 (2019)
12. J. Kaur, A ultimate approach of mitigating attacks in RPL based low power lossy networks, arXiv preprint arXiv:1910.13435 (2019)
13. F.I. Khan, et al., Wormhole attack prevention mechanism for RPL based LLN network, in *Proceedings of the Fifth International Conference on Ubiquitous and Future Networks (ICUFN)* (IEEE, New York, 2013)
14. K. Weekly, K. Pister, Evaluating sinkhole defense techniques in RPL networks, in *Proceedings of the 20th IEEE International Conference on Network Protocols (ICNP)* (IEEE, New York, 2012)
15. F. Ahmed, Y.-B. Ko, Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks. Secur. Commun. Netw. **9**(18), 5143–5154 (2016)
16. J. Granjal, E. Monteiro, J.S. Silva, Enabling network-layer security on IPv6 wireless sensor networks, in *IEEE Global Telecommunications Conference GLOBECOM* (IEEE, New York, 2010)
17. P.N. Mahalle, et al., Identity authentication and capability based access control (IACAC) for the Internet of Things. Journal of Cyber Security and Mobility **1**(4), 309–348 (2013)
18. S. Raza, et al., Securing Internet of Things with lightweight IPsec (2010)
19. S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in *Proceedings of the IETF Workshop on Smart Object Security*, vol. 23 (2012)
20. Top IoT Vulnerabilities, OWASP, Top IoT Vulnerabilities (2016). https://www.owasp.org/index.php/Top_IoT_Vulnerabilities [Retrieved: Sep,2018]
21. D. Conzon, et al., The Virtus middleware: An XMPP based architecture for secure IoT communications, in *Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN)* (IEEE, New York, 2012)
22. J. Granjal, E. Monteiro, J. Silva, Application-layer security for the WoT: extending CoAP to support end-to-end message security for Internet-integrated sensing applications, *International Conference on Wired/Wireless Internet Communication* (Springer, Berlin, 2013)
23. M. Sethi, Arkko, J., Keränen, A., End-to-end security for sleepy smart object networks, in *Proceedings of the 37th Annual IEEE Conference on Local Computer Networks-Workshops* (IEEE, New York, 2012)
24. M. Brachmann, et al., End-to-end transport security in the IP-based Internet of Things, in *Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN)* (IEEE, New York, 2012)
25. A. Reyna, et al., On blockchain and its integration with IoT: Challenges and opportunities. Futur. Gener. Comput. Syst. **88**, 173–190 (2018)
26. M. Banerjee, J. Lee, K.-K.R. Choo, A blockchain future for Internet of Things security: A position paper. Digital Commun. Networks **4**(3), 149–160 (2018)
27. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008)
28. J. Kaur, 10 Blockchain simulators and testnets for all your testing needs, in *Hackernoon* (2020). https://hackernoon.com/blockchain-simulators-ui2030z0 [Retrived: 28 Jan, 2020]
29. G. Wood, Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper **151**, 1–32 (2014)
30. V. Singla, et al., Develop leave application using blockchain smart contract, in *Proceedings of the 11th International Conference on Communication Systems & Networks (COMSNETS)* (IEEE, New York, 2019)
31. J. Kaur, V. Singla, S. Kalra, A Blockchain Based Solution for Securing Data of IoT Devices, in *International Conference on Service-Oriented Computing* (Springer, Cham, 2019)
32. R. Ameer, What Is Hyperledger? The Most Comprehensive Guide Ever!' (2017). https://blockgeeks.com/guides/hyperledger/, [Retrieved: Feb,2019]
33. G. Greenspan, Multichain private blockchain-white paper (2015). http://www.multichain.com/download/MultiChain-White-Paper.pdf.

34. M. Samaniego, R. Deters, Blockchain as a Service for IoT, in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (IEEE, New York, 2016)
35. Popov, Serguei, The tangle. cit (2016), p. 131
36. J. Pan, et al., EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts. IEEE Internet Things J. **6**(3), 4719–4732 (2018)
37. A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in Internet of Things: challenges and solutions. arXiv preprint arXiv:1608.05187 (2016)
38. F. Gilles, W. Bendella, E. Alves, Blockchain-Based Decentralized Cloud Computing, in *iExec Corporation* (2018)
39. Y. Sun, et al., Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment. IEEE Internet Things J. **6**(3), 5791–5802 (2019)
40. K. Jaspreet, A semi supervised hybrid protection for network and host based attacks. J. Eng. Appl. Sci. **12**(12), 3108–3112 (2017)
41. J. Linus, O. Olsson, Improving Intrusion Detection for IoT Networks- A Snort GPGPU Modification Using OpenCL, Master's Thesis (Department of CSE, Chalmers University of Technology and University of Gothenburg, Gothenburg, 2018)
42. A. Sforzin, et al., RPiDS: Raspberry Pi IDS—A Fruitful Intrusion Detection System for IoT, in International IEEE Conferences on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld) (IEEE, New York, 2016)
43. M. Bikash, Do we need only AI or IoT or ML or BlockChain or all of them together? 2(019). http://www.bikashmohanty.com/topics/do-we-need-only-ai-or-iot-or-ml-or-blockchain-or-all-of-them-together.html, [Retrieved: March,2019]
44. Yann300, Remix Documentation-Release 1 (2018). https://buildmedia.readthedocs.org/media/pdf/remix/latest/remix.pdf [Retrieved:Nov,2018]
45. Low Orbit Ion Cannon, Wikipedia: The Free Encyclopedia (2018). https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon [Retrieved: Oct,2018]
46. C. Francois, Keras Documentation (2015). https://keras.io [Retrieved:Dec,2018]
47. Long short-term memory, Wikipedia: The Free Encyclopedia (2018). https://en.wikipedia.org/wiki/Long_short-term_memory [Retrieved: Sep,2018]

ECOM: Epoch Randomness-Based Consensus Committee Configuration for IoT Blockchains

Ronghua Xu, Deeraj Nagothu, and Yu Chen

1 Introduction

With the proliferation of the Internet of Things (IoT), the rapid advancement in Artificial Intelligence (AI) combined with Big Data technology brings smart applications and services to revolutionize human life. By integrating heterogeneous computing platforms and hierarchical edge–fog–cloud networking paradigm, the concept of Smart Cities becomes realistic to provide seamless, intelligent, and safe services for communities and the society [54, 56]. The IoT devices in smart cities are geographically scattered across near-site network edges and managed by fragmented service domains with varying security policies. However, most state-of-the-art smart cities applications heavily rely on a centralized framework which is vulnerable to a single point of failure and faces heterogeneity and scalability challenges with wide adoption of the IoT devices [1].

As the underlying technology of cryptocurrencies like Bitcoin [33], blockchain has demonstrated great potential to revolutionize traditional financial applications and information and communication technology (ICT). In general, the blockchain system utilizes a peer-to-peer (P2P) networking architecture for transactions and blocks propagation. All miners or validators cooperatively execute a cryptographic consensus protocol to maintain a transparent, immutable, and auditable distributed ledger. Thus, blockchain is promising to provide a decentralized and trust-free infrastructure for IoT systems without relying on a reliable centralized third-party authority [46]. Moreover, encapsulating predefines rules into self-executing smart contract (SC) introduces programmability into a blockchain, which can support a

R. Xu · D. Nagothu · Y. Chen (✉)
Department of Electrical and Computer Engineering, Binghamton University, Binghamton, NY, USA
e-mail: rxu22@binghamton.edu; dnagoth1@binghamton.edu; ychen@binghamton.edu

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_7

variety of customized transaction logic rather than simple P2P cash transactions [58].

Recently, leveraging blockchain and smart contract to provide decentralized, verifiable, and traceable IoT-based applications have been among the most intensively studied topics by both academia and industry. There are many reported efforts like public safety service [54] and video surveillance [30, 34] for smart cities, social credit system [50] and time banking application [24, 25, 58], decentralized data markets [47, 55], space situation awareness [53] and avionics management systems [5, 57], biometric imaging data processing [52], and identification authentication and access control [48, 49]. However, directly integrating cryptocurrency-oriented blockchain technologies into IoT systems is hindered by several challenges in terms of scalability, performance, security, and privacy preservation. The blockchain trilemma points out that three important proprieties, decentralization, security, and scalability, cannot perfectly coexist in a blockchain system [62]. Therefore, balancing the trade-offs of the three aspects and selecting the most suitable combination are essential for applying blockchain to complex and large-scale scenes in IoT systems.

The existing popular scaling blockchain solutions aim to address throughput, latency, storage, and networking issues. However, according to heterogeneous system conditions and complicated requirements of domain-specific applications, splitting the whole blockchain network into multiple independent small-scale consensus networks is promising to overcome performance and scalability problems, like Microchain [59] and EconLedger [60]. The rationale is using a periodically random-elected consensus committee to reduce the latency and improve the throughput with less computation and communication overheads on the edge network. However, such a partial decentralized approach is inevitable to reduce security owing to fewer miners or validators participating in consensus protocols. This chapter provides a comprehensive overview of key techniques in epoch randomness generation, network traffic model, and consensus committee configuration to design a secure and efficient committee election mechanism. We introduce ECOM, an epoch randomness-based consensus committee configuration as a case study, and provide experimental results that demonstrate the efficiency and effectiveness of the ECOM scheme.

The rest of this chapter is organized as follows. Section 2 provides an overview of solutions to improve scalability of blockchain systems. The basics of classic epoch randomness and configuration in distributed systems are explained in Sect. 3. Section 4 describes popular network traffic models for data transmission in blockchain. Section 5 introduces an epoch randomness-based committee configuration as a case study on designing a unpredictable random committee election protocol. Section 6 concludes this chapter and summarizes the future research opportunities for IoT blockchain networks.

2 An Overview of Scaling Blockchain Solutions

Scalability and performance are among the key challenges when integrating blockchain into IoT systems. Proof-of-work (PoW) blockchains like Bitcoin suffer high latency and low throughput of processing transactions. Thus, handling a large volume of user data with time-sensitive requirements in IoT applications like smart surveillance is difficult. In addition, processing and storing the complete blockchain data is not suitable for IoT devices with limited storage and computing resources. Furthermore, traditional blockchains use a broadcast manner for data transmission, increasing network resource consumption and propagation delay at the edge.

To improve the scalability and performance of blockchain networks, many different solutions have been proposed to handle the challenges in terms of latency and throughput improvement, storage optimization, and networking efficiency. Figure 1 provides an overview of solutions to scalable blockchain from the perspective of system-level design, consensus implementation, and networking model. According to the hierarchical structure of blockchain, scaling blockchain solutions can be classified as off-chain or on-chain blockchains [62], which are described in the following subsection. At the same time, details of the network traffic model are explained in Sect. 4.

2.1 *Off-Chain Blockchain Solutions*

All off-chain solutions aim at reducing the burden of the main-chain (parent-chain) by off-loading transaction verification or complex and computation-intensive tasks to a sub-chain (child-chain) system. Therefore, off-chains are also called “layer-two” protocols built on “layer-one” blockchains or parent-chains [10].

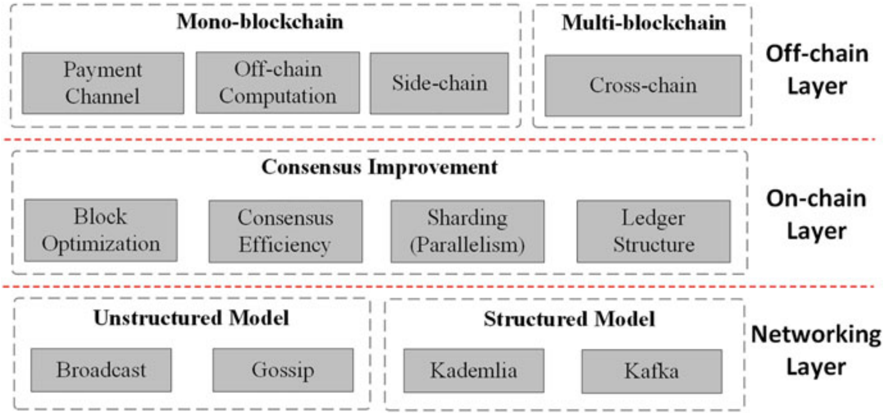


Fig. 1 A layered overview of solutions to scalable blockchains

Payment Channel By establishing a temporary off-chain trading channel to process transactions between parties, payment channel achieves to improve transaction throughput and reduce transaction volume of the main-chain. Lightening network [36] and Raiden Network [39] are representative solutions adopted by Bitcoin and Ethereum separately. However, payment channel requires both parties to be online at the same time to commit transactions or update states of the child-chain.

Side-Chain Similar to payment channel that relies on parent-chain to update transaction status, Pegged Side-Chain [2] is the first side-chain solution that supports atomicity of assets transfer between users within different child-chain of Bitcoin. Plasma [35] is a side-chain platform that uses a smart contract on Ethereum main-chain to record the rules and state of the child-chain. Compared to payment channel, side-chain solutions are not limited to cash payment transaction; it also allows multiple parties to interact with one another without online requirements for all participants.

Off-Chain Smart Contract in Ethereum requires miners to re-execute contract code, and every state, as a result, it is not suitable to run complex and high computational tasks by smart contract. Thus, some off-chain solutions [17, 43] have been proposed to build scalable and complex smart contract-based applications. The task execution and verifiable computation are outsourced to off-chain platform, and only final results and states are submitted back to the main-chain. Thus, side-chain is a promising option for Decentralized Application (DApp) that requires different performance and privacy guarantees. In sum, payment channel, side-chain, and off-chain are deployed as child-chains associated with a monolithic blockchain, like Bitcoin or Ethereum.

Cross-Chain Unlike the mentioned solutions that achieve scalability within a mono-blockchain, cross-chain solutions [6, 45] aim to solve scalability by interconnecting independent blockchains as a multi-blockchain platform. In a cross-chain system, individual blockchain (zone) may execute different consensus algorithms like PoW or Byzantine Fault Tolerant (BFT) to maintain its own distributed ledger, and a hub-chain or relay-chain inter-links heterogeneous zones. An inter-blockchain communication (IBC) protocol allows zones to communicate with one another to exchange values or states.

2.2 *On-Chain Blockchain*

All on-chain solutions focus on performance improvements from perspective of consensus protocol efficiency and chain data optimization.

Block Optimization Bitcoin Cash [4] increases its block size up to 8M, which is 8× than Bitcoin while still maintaining block interval time as 10 min. Increasing block size allows a block to record more transaction such that throughput can be improved with the stable block interval time. However, larger blocks inevitably incur extra overhead on blockchain bandwidth and may lead to mining centralization. Various solutions based on block and transaction compression are proposed to improve the throughput of blockchains, like Txilm [9] and Lumino [22]. Using a hash string with fixed length to represent a raw transaction can reduce some redundant data of a block given majority transactions have been already buffered in the Mempool of miners. Apart from increasing or compressing block data, CUB [51] proposes a scheme that requires each node only store part of the block data to reduce the storage overhead of each node. However, all the abovementioned block data solutions demand more optimization and incentive mechanism to scale the blockchain system.

Consensus Efficiency Various efficient consensus protocols are proposed to improve scalability of blockchains. Bitcoin-NG [11] divides mining time into epochs and a leader responsible for committing transactions into microblocks in current epochs. At the end of an epoch, miners use PoW mechanism to generate a key block, which is only used to select a leader for next epoch. The microblock interval time is much shorter than original PoW block interval time, therefore, it significantly reduces transaction confirmation delay and improves throughput. As an alternative consensus mechanism that reduces energy consumption by PoW, Proof of Stake (PoS) [18] allows miners to use their investment in a blockchain to simulate a verifiable random function to propose new blocks. Owing to computation efficiency and lower block confirmation time, PoS is promising to improve performance and scalability of blockchain. Algorand [15] adopts a hybrid BFT-PoS consensus protocol to achieve high throughput in a 500.000 nodes network.

Sharding Blockchain The sharding blockchains are inspired by the concept of "sharding" [7] in infrastructure of distributed database and cloud. Through securely establishing randomly selected sub-committees (shards), processing of transactions is divided into shards. Thus, shards can perform consensus protocol in parallel to maximize the performance and improve the throughput [44]. SCP [26] firstly incorporates sharding into permissioned BFT blockchain, while Elastico [27] extends SCP to enable a secure sharding protocol for open blockchains. Elastico exhibits almost linear scalability throughput with computation capacity with roughly $O(n)$ message complexity. However, the participants have to download full blockchain data to perform the consensus task, which brings latency in bootstrapping process and storage overload on client nodes.

To enable the parallelization of both network consensus and data storage, a "full sharding" protocol called "OmniLedger" [19] is designed to provide "statistically representative" shards for permissionless transaction processing. OmniLedger uses a bias-resistant protocol called RandHound [42] to generate epoch global randomness strings for sharding committees formation. To optimize trade-off between the number of shards, throughput, and latency, the intra-shard consensus follows an "Optional Trust-but-Verify Validation" model, where optimistic validators make a provisional but unlikely-to-change commitment and core validators subsequently verify again the transactions to provide finality and ensure verifiability [19]. To secure cross-shard transactions, OmniLedger introduces a novel Byzantine Shard Atomic Commit protocol to handle atomically transactions processing across shards. Furthermore, a gradually in-and-out committee members swap strategy could reduce extra message overhead and bootstrapping the latency in shard reconstruction.

Another epoch-based, two-level BFT protocol called RapidChain [61] is proposed for scaling blockchain via full sharding. RapidChain employs block pipelining strategy to achieve very high throughputs in the intra-committee consensus. Furthermore, a novel gossiping protocol for large blocks reduces the large overhead on committee-to-committee communication and ensures an efficient cross-shard transaction verification.

Ledger Structure Unlike the tradition ledger structure of blockchain in which all blocks are organized in a single hash chain, Directed Acrylic Graph (DAG)-based solutions [3, 23, 37] are proposed to revise the ledger structure that allows for concurrent transaction processing to improve throughput. In a DAG ledger, links between data blocks do not follow one-to-one mapping in a chained structure, such that multiple blocks can connect to a parent block. The blocks can be concurrently processed, as a result, more transactions can be recorded in the system. However, existing DAG solutions still rely on proof-of-work (PoW) consensus mechanisms to guarantee the network scalability and mitigate Sybil attacks, and it is hard to further apply on IoT scenarios.

3 Epoch Randomness and Configuration

Among all proposed scalable solutions, sharding scheme provides the most efficient candidate for IoT scenarios by splitting the whole network into parallel small consensus committees that significantly reduce computation, communication, and storage overhead. Epoch randomness generation is an important issue to ensure that all participants are “fairly” elected as committee members under a byzantine network environment. By dynamically choosing nodes to reconfigure consensus committee based on a global randomness mechanism, it can prevent an adversary from concentrating its powers or stakes in a committee and controlling blockchain by exceeding the Byzantine tolerant threshold. In general, a good distributed randomness generation needs to satisfy proprieties, like Public-Verifiability, Bias-Resistance, Unpredictability, and Availability [44]. The following subsections introduce baselines of randomness generation.

3.1 Verifiable Random Function (VRF)

Without the knowledge of the seed s, a pseudorandom oracle $v_i = f_s(x_i)$ is not variable by any party that evaluates f_s at point x_i. However, future output values $v_j = f_s(x_j)$ are not indistinguishable from truly random string anymore, and they can be predictably computed by any party. Verifiable Random Function (VRF) [29] is proposed to provide a new type of pseudorandom oracle which aims to address unverifiability of traditional Pseudo-Random Functions (PRFs). VRF requires that the owner of the seed s publishes a value $v_i = f_s(x_i)$ along with a string $proof_s(i)$. Thus, any party can use $proof_s(i)$ to verify v_i without revealing s. Thus, VRF can guarantee verifiability of a pseudorandom oracle without compromising the unpredictability requirement.

The non-interactive zero-knowledge proof (NIZK) [13] is widely adopted by VRF solutions that need neither interaction nor sharing a guaranteed random string. The owner of f_s only publishes its public key PK as a commitment to the function, such that any party can use PK to verify a proof of correctness $proof_s(i)$ for an output $v_i = f_s(x_i)$ generated by the owner. However, NIZK proof verification requires high communication complexity.

3.2 Verifiable Secret Sharing (VSS)

By dividing secret data s into pieces call shares that are distributed among all participants, secret sharing aims to reconstruct original s if more than a certain threshold of participants can present correct shares. Shamir's secret share protocol [40] is a (t, n) threshold secret sharing scheme based on polynomial interpolation. Given a unique polynomial $q(x) = a_0 + a_1 x \ldots + a_{t-1} x^{t-1}$ with degree (t-1), a dealer splits a secret $s = a_0 = q(0)$ into n points $(x_i, q(x_i))$ where $1 \leq x_i \leq n$ and assigns them to n clients separately. Given any subset of t points, s can be recovered by calculating the coefficients of $q(x)$ through interpolation, while knowledge of less than t of shares cannot calculate $s = g(0)$.

Shamir's secret share protocol assumes that a dealer is honest such that all clients can receive correct shares; it is not suitable for a Byzantine network environment. Moreover, the validity of shares needs an interactive protocol requiring multiple rounds of communication. As a fundamental tool of cryptography and distributed computing, Non-interactive Verifiable Secret Sharing (VSS) [12] is proposed to protect against malicious dealer. Verification mechanism of VSS allows each shareholder to validate its shares, and however, participants cannot verify validity of their received shares.

3.3 Publicly Verifiable Secret Sharing (PVSS)

Unlike VSS that support multi-party verification, Publicly Verifiable Secret Sharing (PVSS) [41] scheme allows any party to verify secret shares from other participants without revealing any information about owner's secret or the shares. The PVSS protocol requires that a group of clients C share random seeds $b_{c \in C}$ along with a set of third-party verifiable proofs $\pi_{c \in C}$. Only a threshold of honest clients can recover random seeds from those valid shares.

In the share distribution phase, for each participant i, a client c uses a (t, n)-secret sharing scheme to produce encrypted share $S_i = E(s_i)$, the commitment A_c, and a non-interactive zero-knowledge proof (NIZK) [13] encryption consistency proof P_i. Thus, participant i can verify received secret shares by using A_c and P_i without revealing any information about the shares or secret. Thus, the invalid shares will be discarded. In the recovery phase, participant i can recover b_c through a Lagrange interpolation if no less than t shares are valid and correctly decrypted. The PVSS can efficiently protect against dishonest clients who might intentionally create and distribute invalid shares to prevent honest participants against recovering the unique and validate secret.

4 Network Traffic Model in Blockchain

Blockchain relies on a P2P network to achieve the node discovery, data transmission, and message exchange for the execution of consensus protocol. Thus, network traffic model is critical for security, privacy, and scalability of a blockchain [10]. In general, P2P communication protocols of the blockchain can be categorized into unstructured or structured models.

4.1 Unstructured P2P Network Model

Gossip broadcast algorithms in P2P network adopt an epidemic-style communication [8] to distribute updates and drive the replicas toward consistency for database maintenance. Bitcoin and Hyperledger fabric use the gossip protocol for transaction and block propagation.

In an epidemic gossip protocol, a node holding updates which will be shared with others is an "infective" node, while a node waits for an update that has not been received is called a "susceptible" node. Specially, a node holding received updates is not willing to spread shares which is defined as a "removed" node. Given required node types in propagation, anti-entropy and rumor-mongering are two models in epidemic process. The anti-entropy only requires infective and susceptible nodes and is considered as *SI* model or simple epidemics model. The rumor-mongering includes nodes of the three types and is recognized as *SIR* model or complex epidemics model.

A modified gossip-based multicast protocol [16] is widely used in P2P network to provide reliable and scalable message dissemination. In push gossip process, a node m within a multicast subgroup g with infectivity $I_g(m)$ gossips to a node n within the network N with susceptibility $S_g(n)$, the expected number of messages sent from m to all n in a round is $I_g(m)S_g(n)$, and the total number of messages sent by m is $I_g(m)\sum_{n\in N} S_g(n)$. Given assumption that each g gossips independently, the expected number of messages sent by m is

$$\sum_{m\in g} I_g(m) \sum_{n\in N} S_g(n). \tag{1}$$

Similarly, we can calculate the expected number of messages received by m in a pull gossip round as

$$\sum_{m\in g} S_g(m) \sum_{n\in N} I_g(n). \tag{2}$$

Unstructured network traffic models rely on randomly selected neighbors as graph rather than a predefined topology. Owing to the unpredictable nature of information dissemination, gossip-based multicast protocol can serve as a robust and reliable data propagation mechanism in case of Churn that nodes frequently failing, quitting, or joining. However, the performance is greatly impacted by the large message overhead in the synchronous communication rounds [21]. The gossip protocol needs the time complexity of $O(logn)$ to ensure that all n nodes become infected with high probability. The communication overhead and propagation latency rise considerably when the number of nodes increases with the growing network size.

4.2 Structured P2P Network Model

The structured P2P network relies on a predefined overlay topology to enable a predictable and deterministic broadcast mechanism. Both Kademlia and Kafka are widely adopted by underlying communication protocol implementation of blockchain. For example, Ethereum uses Kademlia to optimize network routing for node discovery and Hyperledger uses Kafka to support ordering services in BFT consensus process.

Kademlia is a P2P distributed hash table (DHT) with provable and consistency and performance in a fault-prone environment [28]. In the Kademlia, each node has a node ID which is an unique identifier in the L-bit key space. The whole key space can be partitioned into L depth binary tree such that each node is treated as a leaf. Kademlia uses a novel XOR operation to calculate the distance between two nodes.

As XOR is symmetric, the smaller result indicates the closer logic distance between two nodes. The nodes with the same common prefix will be added to a k-bucket, which can be recognized as a sub-tree.

For a node in Kademlia, the routing information is stored in a list of k-buckets, and each k-bucket keeps sorted nodes by time last seen. The k in k-bucket is a system-wide replication parameter (for example, $k = 20$) that assumes that k nodes are unlikely to fail within an hour of each other. All k-buckets use a least-recently seen eviction policy to update the routing table. It is resistant to certain Denial-of-Service (DoS) attacks because an adversary cannot flush routing table by simply flooding the network with new nodes. Kademlia adopts a recursive node lookup algorithm to locate the k closest nodes to a target node ID. The lookup initiator picks $\alpha \geq 1$ nodes from its closest non-empty k-bucket and then sends parallel and asynchronous find node request to them.

Kafka aims to provide a distributed and scalable publish–subscribe messaging system for log management with strong consistency given node crash failures [20]. In Kafka system, a topic defines a stream of messages containing a particular type of payload and is divided into multiple partitions. Each broker only stores one or more of partitions to balance load. A partition corresponds to a logic log which is implemented as a set of segment files with the same size like 1 GB. A message stored in Kafka is addressed by its logical offset in the log rather than an explicit message id. Therefore, it reduces the overhead of maintaining auxiliary, seek-intensive random-access index structures that uses message ids to map actually location [20]. To support efficient data transfer in and out of Kafka, messages are only cached on the underlying file system page cache instead of memory cache in process. This avoids double buffering and allows for efficient implementation on VM-based systems. Moreover, a multi-subscriber model can optimize the network access for consumers.

5 ECOM: An Epoch Randomness-Based Committee Configuration for IoT Blockchains

To enable a reliable decentralized deepfake detection for video–audio surveillance systems [31, 32], EconLedger [60] adopts a novel Proof-of-ENF (PoENF) consensus-based lightweight blockchain for small-scale IoT networks. EconLedger relies on a small random selected consensus committee to improve performance and scalability but at the cost of partial decentralization. Thus, an epoch randomness-based committee configuration (ECOM) is designed and implemented on the EconLedger network to ensure that robustness and security are not sacrificed by a small-scale consensus network including fewer validators.

5.1 ECOM System Design

ECOM works under a permissioned network environment, which provides basic security primitives like public key infrastructure (PKI), identity authentication, and access control. All nodes must finish registration to join the network with authorized access privileges, and therefore, it can prevent against Sybil attacks happened in the open-access network. In general, smart surveillance systems run on a synchronous network condition. Thus, operations and processes in ECOM can be coordinated in rounds with bounded delay constraints. Figure 2 presents a system architecture of ECOM including two main functionalities: (i) epoch randomness generation to ensure unbiasability, unpredictability, and availability of global random seed update and (ii) random committee configuration based on cryptographic scheme.

The epoch randomness is performed by current PoENF committee M at the end of dynasty [60]. Each validator $v_i \in M$ queries the current head of distributed ledger as the chain head and then feeds the hashed value to a pseudorandom number generator to generate a random seed S_i. The PoENF committee utilizes an epoch randomness generation protocol to forge a global epoch random seed S^* based on sum of recoverable and valid random seed S_i. The S^* will be updated across the whole network by a security and efficient P2P propagation mechanism. All nodes use their ID profile and receive S^* to join a random committee election process. Finally, validators of the new committee establish a fully connected P2P consensus network and record the new committee configuration into an epoch block that is finalized on the distributed ledger. Until now, a new dynasty starts, and all nodes

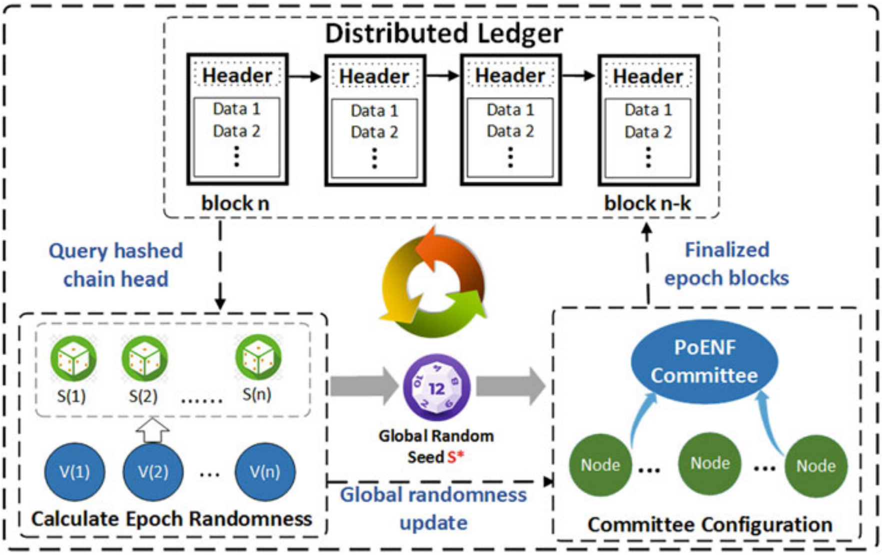


Fig. 2 The system architecture of ECOM

can query the latest epoch block to learn the new committee configuration. The key design and workflows are described as follows.

Epoch Randomness Generation Each validator $v_i \in M$ uses its keypair $(d_i^{SK}, d_i^{PK}) \leftarrow$ **RSA**.**gen**(v_i) that is generated by a trust KPI for digital signature scheme, like **RSA**.**sign** and **RSA**.**ver**. While data communication channels are protected by symmetric encryption **AE**.**enc** and decryption **AE**.**dec** functions. Given assumption that an adversary cannot control more than f validators, current committee size needs to satisfy $m = |M| \geq 3f + 1$. Our epoch randomness generation uses a PVSS scheme, and we let $t = f + 1$ be the secret share threshold to tolerant Byzantine failures.

- *Share Distribution*: each validator v_i chooses a private set of coefficients $\hat{a_i} = (a_{ik})_{k \in [0,t-1]}$, where $a_{ik} \in_R \mathbb{Z}_q^*$ for a large prime q. Then, it uses $\hat{a_i}$ to build a degree of $t - 1$ security sharing polynomial $s_i(x) = \sum_{k=0}^{t-1} a_{ik}x^k$ for (t, m) secret sharing. Let secret $S_i = s_i(0) = a_{i0}$, then t-out-of-m shares for other nodes are computed as $s_i(j)$, where $j \in [1, m]$. To enable NIZK proof, v_i selects a generator G of multiplicative group $\mathcal{G}$ and creates a set of polynomial commitments $\hat{A_i} = (G^{a_{ik}})_{k \in [0,t-1]}$ along with proofs $P_i(j) = G^{s_i(j)}$ associated with shares $s_i(j)$. Afterward, v_i broadcasts encrypted shares $Shares_i(j) =$ **AE**.**enc**$(s_i(j), P_i(j), \hat{A_i})$ along with a signature $\sigma_i(j) \leftarrow$ **RSA**.**sign**$((s_i(j), P_i(j), \hat{A_i}), d_i^{SK})$ to peers v_j such that $i \neq j$.
- *Share Verification*: every validator v_i initializes a bit-vector $\hat{V_i} = (v_{i1}, ..., v_{im})$ to zero, which is used to keep track of valid secrets $s_j(0)$ received. After receiving shares from v_i, each peer v_j validates $\sigma_i(j)$ by checking output of **RSA**.**ver**$(\sigma_i(j), d_i^{PK})$. If $\sigma_i(j)$ is valid, it decrypts shares $(s_i(j), P_i(j), \hat{A_i}) \leftarrow$ **AE**.**dec**$(Shares_i(j))$ and saves them for consistency check and recovery round. Each validator v_i uses buffered $\hat{A_j}$ to verify if each $s_j(x)$ is valid. The verification process is done by checking that $S_j(x) = G^{s_j(x)}$ where

$$S_j(x) = \prod_{k=0}^{t-1} A_{jk}^{x^k} = G^{\sum_{k=0}^{t-1} a_{jk}x^k} = G^{s_j(x)}. \tag{3}$$

  Given verification results of $s_j(x)$, v_i launches a Byzantine Agreement (BA) voting process to finalize the consistency of shares used for recovering $s_j(0)$. During the *prepare* stage, each v_i broadcasts the message $(p, i, j, 1)$ as a positive vote on $s_j(0)$ if $s_j(i)$ is valid, where flag p means *prepare* stage. Otherwise, the client broadcasts message $(p, i, j, 0)$ as a negative vote.
- *Share Commitment:* for the *commit* stage, until at least $2f + 1$ positive *prepare* votes are received for secret $s_j(0)$, v_i broadcasts $(c, i, j, 1)$ as a positive commitment, where the flag c indicates the *commit* stage. If there are at least $f + 1$ negative *prepare* votes for secret $s_j(0)$, v_i broadcasts $(c, i, j, 0)$ as a negative commitment. Finally, if there are at least $2f + 1$ positive commitment votes for secret $s_j(0)$, validator v_i finalizes the consistency of shares by setting $v_{ij} = 1$

in $\hat{V}_i$, which indicates that the secret $s_j(0)$ is recoverable if at least t validators survive at recovery round.

- *Randomness Recovery:* each validator i checks v_{ij} in $\hat{V}_i$ and puts all 1-entry of j into a set of recoverable nodes M'. If $m' = |M'| \geq t$, v_i broadcasts $s_j(i)$ and M' to all peers for $s_j(0)$ recovery. Once at least t shares for each $j \neq i$ have arrived, validator v_i can reconstruct the secret sharing polynomial $s_j(x)$ through a Lagrange interpolation and compute the secret $s_j(0)$. Finally, the global random seed can be computed:

$$S^* = \bigoplus_{j=1}^{m'} s_j(0), m' > f. \tag{4}$$

Because all honest validators of consensus committee have the same set M', they can make agreement on a unique global random seed S^*

Random Committee Configuration Given a small-scale EconLedger network including $u_i \in N$ nodes, each node u_i uses its credit stake $0 \leq c_i \leq C_{max}$ to participant new committee election. The committee configuration relies on a VRF-based cryptographic sortition scheme [15] that chooses a random subset of nodes as committee according to per-node's credit stake. The total credit of all nodes is $C = \sum_1^n c_i$, where $n = |N|$, the probability that node i becomes a member of the new committee is proportional to c_i/C. Let current epoch randomness $S_e = S^*$, then each node u_i will be assigned a Virtual ID VID_i as

$$(VID_i, \pi_i) = VRF_{d_i^{SK}}(S_e||v_i), \tag{5}$$

where VRF is a verifiable random function, π_i is a verifiable string for VID_i, and v_i is identity information of u_i.

To select committee members in proportion to their credits, each unit of credit is considered as a different "sub-node." If node i owns c_i (integral) units of credit, the simulated node (i, j) with $j \in \{1, \ldots, c_i\}$ represents the jth unit of credit that node i owns, and node i is selected with probability $p = \frac{\tau}{C}$, where τ specifies a threshold to determine the expected number of nodes selected for final committee. The VID_i generated by Eq. (5) could be used to determine how many sub-nodes are selected. Since the probability that exactly k out of the c (the node's credit) sub-nodes are selected follows the binomial distribution, $B(k; c, p) = \binom{c}{k} p^k (1-p)^{c-k}$, where $\sum_{k=0}^{c} B(k; c, p) = 1$. The sortition algorithm first divides the interval [0,1) into consecutive intervals I^j defined as form:

$$I^j = \left[\sum_{k=0}^{j} B(k; c, p), \sum_{k=0}^{j+1} B(k; c, p) \right], j \in \{1, \ldots, c_i\}. \tag{6}$$

Given interval I^j in which $VID_i/2^L$ (where L is the bit-length of hashed VID string) falls, the number j will be used to represent how many of a node's c sub-nodes are selected. By using a biased resistant global epoch random seed S_e, the VID generated by VRF defined in Eq. (5) is essentially uniformly distributed between 0 and $2^L - 1$. Without knowing private key d_i^{SK}, an adversary cannot predicate if a node u_i is chosen or not. Thus, the committee members are selected at random according to nodes' credits.

5.2 Prototype Implementation

To verify the proposed ECOM, a concept-proof prototype is implemented in Python. The networking and web service APIs by client and server are developed by using Flask [14], which is a light micro-framework for Python application. All cryptographic functions are developed on the foundation of standard python lib: cryptography [38], and we use RSA for key generation and digital signature while using SHA-256 for all hash operations.

Table 1 describes the devices used for the experimental study. All devices run on the local area network (LAN) to simulate a small-scale smart surveillance network. The Dell Optiplex-7010 manages node information and acts as a bootstrap node to initialize a Kademlia P2P network, while 20 Raspberry Pis (RPis) simulate IoT devices, which can work as nodes or validators to perform PoENF consensus algorithm and ECOM protocol.

5.3 Performance Evaluation

To evaluate the latency of the running ECOM including both the round trip time (RTT) and service processing time on the local host, a set of experiments is conducted by executing multiple complete rounds of ECOM consensus protocol. We conducted 100 Monte Carlo test runs and used the average of results for evaluation. The computation costs by message encryption and decryption are not considered during the test. As BA voting process requires a majority condition of

Table 1 Configuration of experimental nodes

Device	Dell Optiplex-7010	Raspberry Pi 4 Model B
CPU	Intel Core TM i5-3470 (4 cores), 3.2 GHz	Broadcom ARM Cortex A72 (ARMv8), 1.5 GHz
Memory	8 GB DDR3	4 GB SDRAM
Storage	350G HHD	64 GB (microSD card)
OS	Ubuntu 16.04	Raspbian GNU/Linux (Jessie)

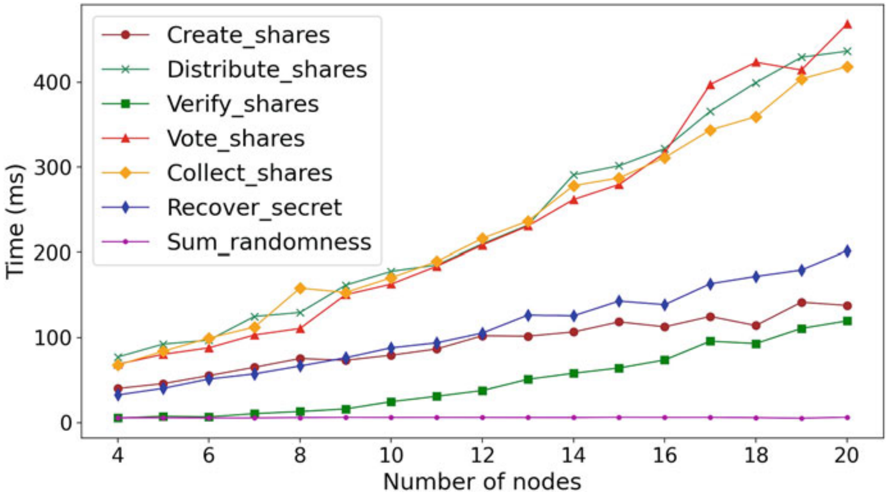


Fig. 3 Latency for completing one round of epoch randomness generation with different validators. Each line represents time delay incurred by single step in protocol

$n \geq 3f + 1$, the minimum committee size is 4. Figure 3 presents the latency caused by completing an entire round of epoch randomness generation given the number of validators (committee size) varying from 4 to 20.

In Create_shares step, each validator locally computes t-out-of-n Shamir secret shares of a random seed b with computation complexity $\mathcal{O}(n+t)$. Thus, the latency is almost linear scale to n, and it varies from 40 ms to 138 ms. Like secret shares generation, Verify_shares and Sum_randomness steps only process received shares with complexity $\mathcal{O}(n)$, and their delays are almost linear scale to n. Compared with Sum_randomness which simply sums a set of recovered random seeds to generate an epoch random seed, Verify_shares involves more mathematical operations, like modular multiplication for NIZK proofing. Therefore, the Verify_shares step incurs longer delay than Sum_randomness does. During Recover_shares step, a validator reconstructs each secret by computing Lagrange basis polynomials in time $\mathcal{O}(n)$. As a result, it requires computation cost $\mathcal{O}(n^2)$ in total to recover all n secrets. As Fig. 3 illustrates, line of Recover_shares introduces more latency as increasing nodes than Verify_shares does.

In Distribute_shares step, each validator sends shares to $n-1$ participants, so that the communication latency becomes dominant without considering encryption and decryption overhead. Given $\mathcal{O}(n)$ communication complexity for each validator, network latency of Distribute_shares varies from 77 ms to 436 ms as nodes scale from 4 up to 20. As Vote_shares and Collect_shares steps also incur communication complexity $\mathcal{O}(n)$ by sending voting messages and verifying shares, their delays have the almost same scaling trend as Distribute_shares shows in Fig. 3. Given results shown in Fig. 3, we can calculate the total network latency of executing an epoch randomness generation round, which varies from 0.3 s to 1.7 s as nodes scale from 4 up to 20.

5.4 Security Analysis

Given the assumption that honest validators follow the protocol and cryptographic primitives can provide their intended security properties, the secret sharing threshold $t = f + 1$ can prevent dishonest peers from recovering the honest nodes' secrets before the barrier. Thus, our epoch randomness generation can ensure unbiasability. In addition, calculating global random seed S^* requires $m' \geq f + 1$ recoverable secrets such that at most f are from malicious peers. Given that at least one random seed is shared by the honest validator, unpredictability of the epoch random seed is guaranteed. Furthermore, assuming that the secret sharing threshold $t = f + 1$ as well as no collaboration between the dishonest nodes, availability is ensured because $f + 1$ honest nodes out of the total $2f + 1$ positive voters are able to recover the secrets.

We assume that an adversary can control no more than $\lfloor \frac{n}{3} \rfloor$ of committee members, and therefore, honest validators can correctly maintain agreed epoch random seeds. The security of committee configuration mechanism can be modeled as a random sampling problem with two possible outputs: honest or malicious. Given assumption that potential nodes are infinite, the power of adversary follows the binomial distribution in form of (Eq. (7)):

$$P\left[X \leq \lfloor \frac{n}{3} \rfloor\right] = \sum_{k=0}^{n} \binom{n}{k} m^k (1-m)^{n-k}. \tag{7}$$

Owing to unpredictable epoch random seed generation, each committee formation based on a VRF-based sortition scheme is complete random. Therefore, an adversarial has at most $m = 0.25$ probability of controlling a single round committee selection. As a result, the probability that an adversary controls n consecutive committee formation is upper-bounded by

$$P[X \geq n] = \frac{1}{4^n} < 10^{-\lambda}. \tag{8}$$

Let system security parameter $\lambda = 6$, then an adversary can control at most 10 consecutive committee election rounds with high probability.

6 Conclusions

This chapter reviews the basics of improving performance and scalability in blockchain systems. Given a comprehensive overview of scaling blockchain solutions, epoch randomness mechanism and network traffic model are evaluated and recognized as key challenges in designing parallel small-scale consensus networks for heterogeneous IoT scenarios. In addition, ECOM is introduced as a case study that demonstrates how epoch randomness generation and committee selection can guarantee the robustness and security of a small-scale consensus committee under a Byzantine network environment.

ECOM is a promising solution to enable unpredictable random committee configuration and mitigate reduced security by fewer validators. However, several open issues remain in developing a practical solution in real-world IoT systems. Although PVSS-based epoch randomness generation can achieve efficiency in a small-scale network, more investigation and test are needed to evaluate how epoch random seed propagation latency and coverage are influenced by the network size. Another challenge is designing a hybrid P2P communication mechanism by combining unstructured and structured models, which greatly impacts performance and security in IoT blockchains.

References

1. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the Internet of Things: A comprehensive survey. IEEE Commun. Surv. Tutorials **21**(2), 1676–1717 (2018)
2. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, P. Wuille, Enabling blockchain innovations with pegged sidechains, vol. 72 (2014). http://www.opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains
3. L. Baird, The Swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance. Swirlds Tech Reports SWIRLDS-TR-2016-01, Tech. Rep (2016)
4. Bitcoin Cash. https://bitcoincash.org/, accessed: Dec. 22 2021
5. E. Blasch, R. Xu, Y. Chen, G. Chen, D. Shen, Blockchain methods for trusted avionics systems, in *Proceedings of the 2019 IEEE National Aerospace and Electronics Conference (NAECON)* (IEEE, New York, 2019), pp. 192–199
6. Cosmos. https://v1.cosmos.network/resources/whitepaper, accessed: Dec. 22 2021
7. K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E.G. Sirer, et al.: On scaling decentralized blockchains, in *International Conference on Financial Cryptography and Data Security* (Springer, Berlin, 2016), pp. 106–125
8. A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, D. Terry, Epidemic algorithms for replicated database maintenance, in *Proceedings of the sixth annual ACM Symposium on Principles of distributed computing* (1987), pp. 1–12
9. D. Ding, X. Jiang, J. Wang, H. Wang, X. Zhang, Y. Sun, Txilm: Lossy block compression with salted short hashing. arXiv preprint arXiv:1906.06500 (2019)
10. M. Dotan, Y.A. Pignolet, S. Schmid, S. Tochner, A. Zohar, Survey on blockchain networking: Context, state-of-the-art, challenges. ACM Comput. Surv. (CSUR) **54**(5), 1–34 (2021)
11. I. Eyal, A.E. Gencer, E.G. Sirer, R. Van Renesse, Bitcoin-ng: A scalable blockchain protocol, in *Proceedings of the 13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)* (2016), pp. 45–59
12. P. Feldman, A practical scheme for non-interactive verifiable secret sharing, in *Proceedings of the 28th Annual Symposium on Foundations of Computer Science (SFCS 1987)* (IEEE, New York, 1987), pp. 427–438
13. A. Fiat, A. Shamir, How to prove yourself: Practical solutions to identification and signature problems, in *Conference on the Theory and Application of Cryptographic Techniques* (Springer, Berlin, 1986), pp. 186–194
14. Flask: A Python Microframework. http://flask.pocoo.org/, accessed: Dec. 22 2021

15. Y. Gilad, R. Hemo, S. Micali, G. Vlachos, N. Zeldovich, Algorand: Scaling byzantine agreements for cryptocurrencies, in *Proceedings of the 26th Symposium on Operating Systems Principles* (ACM, New York, 2017), pp. 51–68
16. K. Jenkins, K. Hopkinson, K. Birman, A gossip protocol for subgroup multicast, in *Proceedings 21st International Conference on Distributed Computing Systems Workshops* (IEEE, New York, 2001), pp. 25–30
17. H. Kalodner, S. Goldfeder, X. Chen, S.M. Weinberg, Felten, E.W., Arbitrum: scalable, private smart contracts, in *Proceedings of the 27th {USENIX} Security Symposium ({USENIX} Security 18)* (2018), pp. 1353–1370
18. A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in *Annual International Cryptology Conference* (Springer, Berlin, 2017), pp. 357–388
19. E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, B. Ford, Omniledger: a secure, scale-out, decentralized ledger via sharding, in *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)* (IEEE, New York, 2018), pp. 583–598
20. J. Kreps, N. Narkhede, J. Rao, et al. Kafka: a distributed messaging system for log processing, in *Proceedings of the NetDB*, vol. 11 (2011), pp. 1–7
21. L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, Y. Yang, A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling. ACM Comput. Surv. (CSUR) **53**(1), 1–32 (2020)
22. S.D. Lerner, R.S.K. Chief Scientist, Lumino Transaction Compression Protocol (LTCP) (2017)
23. Y. Lewenberg, Y. Sompolinsky, A. Zohar, Inclusive block chain protocols, in *International Conference on Financial Cryptography and Data Security* (Springer, Berlin, 2015), pp. 528–547
24. X. Lin, R. Xu, Y. Chen, J. Lum, Enhance generalized exchange economy using blockchain: a time banking case study, in *The IEEE Blockchain Technical Briefs* (2019)
25. X. Lin, R. Xu, Y. Chen, J.K. Lum, A blockchain-enabled decentralized time banking for a new social value system, in *Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS)* (IEEE, New York, 2019), pp. 1–5
26. L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, P. Saxena, SCP: A computationally-scalable byzantine consensus protocol for blockchains. https://www.weusecoins.com/assets/pdf/library/SCP (2015)
27. L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, P. Saxena, A secure sharding protocol for open blockchains, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (ACM, New York, 2016), pp. 17–30
28. P. Maymounkov, D. Mazieres, Kademlia: A peer-to-peer information system based on the XOR metric, in *International Workshop on Peer-to-Peer Systems* (Springer, Berlin, 2002), pp. 53–65
29. S. Micali, M. Rabin, S. Vadhan, Verifiable random functions, in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (cat. No. 99CB37039)* (IEEE, New York, 1999), pp. 120–130
30. D. Nagothu, R. Xu, S.Y. Nikouei, Y. Chen, A microservice-enabled architecture for smart surveillance using blockchain technology, in *Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2)* (IEEE, New York, 2018), pp. 1–4
31. D. Nagothu, R. Xu, Y. Chen, E. Blasch, A. Aved, Defake: Decentralized ENF-consensus based deepfake detection in video conferencing, in *Proceedings of the IEEE 23rd International Workshop on Multimedia Signal Processing, Tampere, Finland* (2021), pp. 6–8
32. D. Nagothu, R. Xu, Y. Chen, E. Blasch, A. Aved, Detecting compromised edge smart cameras using lightweight environmental fingerprint consensus, in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems* (2021), pp. 505–510
33. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, in *Decentralized Business Review* (2008), p. 21260
34. S.Y. Nikouei, R. Xu, D. Nagothu, Y. Chen, A. Aved, E. Blasch, Real-time index authentication for event-oriented surveillance video query using blockchain, in *Proceedings of the 2018 IEEE International Smart Cities Conference (ISC2)* (IEEE, New York, 2018), pp. 1–8

35. J. Poon, V. Buterin, Plasma: Scalable autonomous smart contracts, in *White Paper* (2017), pp. 1–47
36. J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments (2016). https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf, accessed: Dec. 22 2021
37. S. Popov, The tangle. White Paper **1**(3), 1–28 (2018)
38. pyca/cryptography documentation. https://github.com/pyca/cryptography, accessed: Dec. 22 2021
39. Raiden Network. https://raiden.network/, accessed: Dec. 22 2021
40. A. Shamir, How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
41. M. Stadler, Publicly verifiable secret sharing, in *International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, Berlin, 1996), pp. 190–199
42. E. Syta, P. Jovanovic, E.K. Kogias, N. Gailly, L. Gasser, I. Khoffi, M.J. Fischer, B. Ford, Scalable bias-resistant distributed randomness, in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)* (IEEE, New York, 2017), pp. 444–460
43. J. Teutsch, C. Reitwießner, A scalable verification solution for blockchains. arXiv preprint arXiv:1908.04756 (2019)
44. G. Wang, Z.J. Shi, M. Nixon, S. Han, SOK: Sharding on blockchain, in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (2019), pp. 41–61
45. G. Wood, Polkadot: Vision for a heterogeneous multi-chain framework. White Paper **21**, 2327–4662 (2016)
46. J. Xie, F.R. Yu, T. Huang, R. Xie, J. Liu, Y. Liu, A survey on the scalability of blockchain systems. IEEE Netw. **33**(5), 166–173 (2019)
47. R. Xu, Y. Chen, Fed-ddm: A federated ledgers based framework for hierarchical decentralized data marketplaces, in *Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN)* (2021)
48. R. Xu, Y. Chen, E. Blasch, G. Chen, BlendCAC: A blockchain-enabled decentralized capability-based access control for IoTs, in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (IEEE, New York, 2018), pp. 1027–1034
49. R. Xu, Y. Chen, E. Blasch, G. Chen, BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the IoT. Computers **7**(3), 39 (2018)
50. R. Xu, X. Lin, Q. Dong, Y. Chen, Constructing trustworthy and safe communities on a blockchain-enabled social credits system, in *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (ACM, New York, 2018), pp. 449–453
51. Z. Xu, S. Han, L. Chen, Cub, a consensus unit-based storage scheme for blockchain system, in *Proceedings of the 2018 IEEE 34th International Conference on Data Engineering (ICDE)* (IEEE, New York, 2018), pp. 173–184
52. R. Xu, S. Chen, L. Yang, Y. Chen, G. Chen, Decentralized autonomous imaging data processing using blockchain, in *Multimodal Biomedical Imaging XIV*, vol. 10871 (International Society for Optics and Photonics, Bellingham, 2019), p. 108710U
53. R. Xu, Y. Chen, E. Blasch, G. Chen, Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. Opt. Eng. **58**, 58–58–16 (2019). https://doi.org/10.1117/1.OE.58.4.041609
54. R. Xu, S.Y. Nikouei, Y. Chen, E. Blasch, A. Aved, BlendMAS: A blockchain-enabled decentralized microservices architecture for smart public safety, in *Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain)* (IEEE, New York, 2019), pp. 564–571
55. R. Xu, G.S. Ramachandran, Y. Chen, B. Krishnamachari, BlendSM-DDM: Blockchain-enabled secure microservices for decentralized data marketplaces, in *Proceedings of the 2019 IEEE International Smart Cities Conference (ISC2)* (IEEE, New York, 2019)

56. R. Xu, S.Y. Nikouei, D. Nagothu, A. Fitwi, Y. Chen, BlendSPS: A blockchain-enabled decentralized smart public safety system. Smart Cities **3**(3), 928–951 (2020)
57. R. Xu, Y. Chen, E. Blasch, G. Chen, A. Aved, D. Shen, Hybrid blockchain-enabled secure microservices fabric for decentralized multi-domain avionics systems, in *Sensors and Systems for Space Applications XIII*, vol. 11422 (International Society for Optics and Photonics, Bellingham, 2020), p. 114220J
58. R. Xu, Z. Zhai, Y. Chen, J.K. Lum, Bit: A blockchain integrated time banking system for community exchange economy, in *Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2)* (IEEE, New York, 2020), pp. 1–8
59. R. Xu, Y. Chen, E. Blasch, Microchain: A light hierarchical consensus protocol for IoT systems, in *Blockchain Applications in IoT Ecosystem* (Springer, Berlin, 2021), pp. 129–149
60. R. Xu, D. Nagothu, Y. Chen, EconLedger: A proof-of-ENF consensus based lightweight distributed ledger for IoVT networks. Future Internet **13**(10), 248 (2021)
61. M. Zamani, M. Movahedi, M. Raykova, Rapidchain: Scaling blockchain via full sharding, in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (ACM, New York, 2018), pp. 931–948
62. Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: A survey. IEEE Access **8**, 16440–16455 (2020)

Customer Outcome Framework for Blockchain-Based Mobile Phone Applications

Melissa Liow, Li Sa, and Yeap Peik Foong

1 Introduction

Blockchain-based mobile phone applications (BMPAs) have been growing rapidly in the digital economy. Along with the increase in BMPA users, the number of businesses accepting blockchain-based mobile payment modes is on the rise. BMPAs present great opportunity for businesses to increase their selling of products and forge customer loyalty. BMPAs chronologically record transactions and track assets through shared distributed ledgers in a network. The functions of BMPAs include making a reservation, booking a flight or a hotel room, entering into a contractual agreement, sending and receiving money, and making payments for products and services [1]. This technology permits trailing the ownership of assets and the right to use when leased to a third party. Anything of value can be recorded, trailed, leased, and exchanged on BMPAs. Replica records of these transactions are seamlessly shared with participating agents in a network. While BMPA technology is still in its embryonic stages, airlines, hotels, restaurants, travel agencies, and other retail businesses find that by embracing the blockchain technology in their operations, the stakeholders will collectively gain value from its usage.

Most of the blockchains are linked with cryptocurrencies. While blockchains are mostly public, the participants' identity is kept anonymous throughout the transactions. A business blockchain does not necessarily need any cryptocurrency, such as Litecoin, Ethereum, and Bitcoin, and is therefore kept private. Permission is required to access the distributed ledger, and the level of permission can vary

M. Liow · L. Sa
PSB Academy, Singapore, Singapore
e-mail: melissa.liow@psb-academy.edu.sg

Y. P. Foong (✉)
University of Newcastle, Callaghan, NSW, Australia
e-mail: peikfoong.yeap@newcastle.edu.au

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_8

depending on the participants' role in the network. Despite the complexity of blockchain technology, the implications for the industries can be positive and long-standing for improving customer satisfaction, service quality, customer loyalty, repeat purchases, and profitability [1]. Its essential features have the potential to revolutionize many business aspects. The cryptographic security, tamper-free, and trust-evident structure can develop decentralized autonomous businesses, create smart contracts, digitalize fiat currencies, and offer many more applications. Hospitality businesses pursue the likelihood of digitalizing fiat currencies, the likes of Expedia.com, Travloka.com, TUI Group, and BitcoinSky. The process becomes quicker, and transactions are secured through disintermediation, which in turn reduces the processing costs [1].

Researchers have criticized BMPA in many ways, from user interfaces to overwhelming sites and from mobile phone applications to an overemphasis on promotional efforts at the expense of content [1–3]. These factors are likely important contributors, but the more likely cause is the lack of understanding of the firm's targeted markets. Scholars argue that e-commerce, social media, and mobile commerce should consider the desired value or motivations behind consumer use of the sites or mobile phone applications [4, 5]. Shoppers tend to select and return to retailers who provide superior value. Therefore, retailers must develop and offer value propositions that are most tempting to customers.

Value judgments are the most important predictors of preference, satisfaction, customer loyalty, and repeat customers' usage or purchase intention [6]. Many scholars assert that trust between the retailers and customers is critical to encourage their initial and continuous patronage [7, 8]. Many extant studies investigated these constructs in the context of offline consumer behavior and the online shopping behavior in e-commerce sites. In terms of customers shopping using BMPAs, empirical research has begun to appear in the marketing literature. Yet, many unanswered questions still linger, including whether the offline and online customer values and trust dimensions recognized in the retailing literature are likewise relevant within the BMPA context. If so, to what degree these differences in value dimensions influence their identification with the BMPA and its customers' future usage.

Therefore, the first objective in this chapter is to conduct a literature review that identifies a suitable overarching research philosophy for BMPA. The literature related to blockchain technology, AI, and mobile phone applications would give researchers insights to understand why individuals continue to use the BMPAs when purchasing goods and services through three lenses: the means-end chain theory, social identity theory, and prospect theory. The second objective in this chapter is to develop a Customer Outcome Framework designed for businesses that adopt BMPAs. The proposed framework will be multidimensional in nature. The third objective in this chapter is to improve the understanding of how utilitarian and hedonic values, trustworthiness, BMPA identification, and perceived risk differ in terms of influencing the repeat customers' usage of BMPAs. The overall aim is to understand customer shopping behavior in the BMPA environment.

We endeavor to discuss in the context of Singapore because it is a financial hub in Asia, and it has been striving to be the first mover in forming an electronic payment society in Asia. It all started with its online General Interbank Recurring Order (GIRO) system back in 1984. Today, the nation boosts a high mobile payment rate among the young and old. A Smart Financial Centre was setup to rollout FinTech nationwide that shows the serious commitment of the government to achieving the Smart Nation vision. The vision has driven the surge of applying blockchain and artificial intelligence (AI) technologies that help ease business transactions. These digital wallets had broadly improved people's lives in this island city. Therefore, the high level of digital inclusion of Singapore's society makes the nation a suitable research ground for studies regarding BMPAs and its consumer behavior.

2 Literature Review

A review of the extant studies and Singapore's online government sites found that stakeholders across different industries aim to invest in the *right* BMPA technology that benefits their customers. Singapore's electronic payment journey will be presented, which played an integral part in educating users and inculcating responsible online purchasing behavior through secured channels. Singapore government agencies, business merchants, its banking and finance industry, and users form the electronic payment community of Singapore's Smart Nation vision. Blockchain and AI have become one of the most formidable pairs applied in the metaverse, complementing one another's strengths and weaknesses. The technology pair provides personalized services to users and at the same time protects customers' personal biodata. Some of the observable benefits with this powerful pair enable precise data mining for the business community and into improving people's lives. The number of users participating in the mobile payment is increasing, and by integrating the blockchain and AI with the mobile phone payment applications, this chapter introduces the blockchain-based mobile phone applications (BMPAs). This is followed by a critical review of relevant literature from 1991 to 2021. The literature review is performed through the following three lenses: means-end chain theory, social identity theory, and prospect theory.

2.1 Singapore's Electronic Payment Journey

The Monetary Authority of Singapore, MAS [9], stated that electronic payments have been around in Singapore since the mid-1980s. It started with GIRO, which is a cashless, paperless, and convenient payment method that allows users to make worry-free payments to billing organizations via their bank accounts. FAST (Fast and Secure Transfers) was a new electronic fund transfer service launched in 2014. FAST permits account holders of the participating banks to instantly transfer local currency from one bank to another bank. Digital wallets are projected to overtake credit cards by 2024 amid the e-commerce boom, and the lingering COVID-19 pandemic had seen its popularity soar. It was cited in The New Straits Times (March 3, 2021) e-article and report from the Worldpay from FIS [10] pertaining to the latest global payments that bank transfers constitute 12%, followed by digital wallets (20%) and credit cards (45%) in 2020. These are also the three most pervasive online payment methods in Singapore. Electronic payments offer users an efficient and swift method to pay, thus helping businesses to increase productivity. Singapore's Smart Nation vision has been the primary driver that is harnessing blockchain and artificial intelligence (AI) technologies to improve people's lives. The convergence of blockchain and AI can delve in machine learning and empower AI to create and trade financial products. Blockchain technology permits secured sharing and storage of data or anything of value, and AI can perform data mining to generate insights of online customer behavior for value creation. The Smart Financial Centre was setup by MAS to roll out FinTech nationwide. Electronic payment is one of the top items in the Smart Financial Centre's agenda. The MAS vision is to produce an electronic payment society not only to increase users' convenience but also to drive innovation and address market competition. This is where Singapore's BMPA journey started till the present date. MAS plays a pivotal role in *Singapore Payments Roadmap*. It is the central bank and the financial regulatory authority of Singapore. MAS formulates strategies and infrastructure, develops policies, cooperates with industries, and enables an innovative and competitive payment ecosystem that is secure and safe. MAS aims for an inclusive electronic payment society where electronic payment becomes accessible and user-friendly for everyone. MAS works together with KPMG on the Singapore Payments Roadmap to create an efficient payment ecosystem in Singapore. There was a survey conducted by KPMG with more than 2500 stakeholders in the local payment ecosystem. The goal is to understand the present state of how business merchants and consumers make payments. Based on the recommendations constituted in the Singapore Payments Roadmap, the Payments Council was formed by MAS to drive collaboration, innovation, and adoption of electronic payments in the industry. The council was headed by the MAS Managing Director and other stakeholders, including business merchants, banks, trade associations, and payment service providers. The new Payment Services Act or PS Act was passed by the Parliament in 2019. The act streamlines and unifies the regulatory requirements for the range of payment services, including electronic payments, in Singapore. The PS Act embraces a risk-focused and a modular methodology to adhere MAS' rules regarding the scope and risks of every payment service. It allows MAS to respond quickly and be nimble to the evolving payments landscape. Overall, maintaining stability and facilitating growth and innovation of electronic payments in Singapore are paramount.

The nationwide electronic payment options were updated in 2021. These include the Singapore Quick Response Code (SGQR), PayNow, and PayNow Corporate [11]. These electronic payments were established in the Singapore market since 2019, and the growth in the volume and value has been going strong. Alongside debit and credit card transaction volumes and values being stable between 2019 and

2021, the PayNow volumes and values have doubled in 2020 and continued to grow strongly in 2021. Therefore, the use of digital wallet has been expanding among end customers. The SGQR take-up rate has grown from 42 thousand merchant acceptance points in 2019 to 120 thousand and over 260 thousand in 2020 and 2021, respectively. There are presently more than 150 thousand (or 75%) merchants in Singapore that have accepted SGQR as a payment mode. Other than retail stores in the shopping centers, the adoption of SGQR is widespread in hawker centers. The Hawkers Go Digital campaign was introduced in 2020 to further promote the adoption of SGQR into the nation's heartlands. More than 11,000 stalls islandwide made close to $18.3 million, which was close to two million electronic payment transactions (over 94% is made via SGQR) in August 2021 alone. Overall, an interoperable infrastructure has been put into a system that permits low cost, secure, safe, and convenient electronic payments for multiple payment service providers in Singapore. The SG Digital Office (SDA) and the InfoComm Media Development Authority (IMDA) recently collaborated to work on NETSBIZ app. This app allows stallholders to track their payment transactions. Enhancement features including a clear audio alert for incoming transactions in the hawker environment and the use of color to highlight the latest transactions and check against fraudulent transactions are some of the plans in the pipeline [12].

A recent Visa Digital Inclusion Research was conducted by EUGINE Insights in 2021 (Visa Inc., 1996–2021). Two hundred Singaporean and permanent residents between 50 and 80 years of age have participated in the survey. The study aimed to explore the accessibility and literacy of e-commerce services and digital payments among the seniors in Singapore. It was found that 36% of the seniors have done online shopping in the past 1 year compared with 25% in 2018. The top online purchases encompass cleaning or household products (63%), food and groceries (68%), and clothing (69%). Thirty percent of the seniors prefer shopping online than visiting physical brick-and-mortar stores. This trend of digital adoption is likely to accelerate with the COVID-19 pandemic amid the concerns, such as hygiene and safe-distancing measures. This is a confident image of Singapore seniors to partake in the move towards digital-first experiences. Factors such as the ability to shop from the comfort of his or her home (63%), ease of use (64%), and convenience (79%) have driven higher e-commerce surfing rates among this market segment in Singapore. Being the global leader in digital payments, Visa Inc. [13] is committed to advancing digital inclusion so that no one gets left behind. It deems that more work is necessary to change the behaviors of those who have not applied and experienced electronic payment. While the seniors are more aware of the use of digital wallets, Visa Inc. identifies that more education for this group of consumers is needed so that they can enjoy the secure and seamless digital payment experiences. According to the study, seniors in Singapore are familiar with mobile contactless payments (56%), QR code payments (67%), and contactless card payments (90%). Twenty-two percent, 31%, and 68% of the seniors have used QR code payments, made mobile contactless payments, and contactless card payments, respectively. Fifty percent of the seniors cited that they would continue to make digital payments post-COVID-19, and 37% of them prefer to go to business merchants that accept digital payment methods.

2.2 Blockchain and AI Combination in the Metaverse

Jeon et al. [14] described the metaverse as a virtual world that goes beyond reality. Blockchain and AI have significantly contributed to the creation of the virtual world. The demand for virtual reality increases during the pandemic and endemic stages of the COVID-19; therefore the industry representing the metaverse is expanding. This section explains how blockchain and AI impact the metaverse. The term metaverse is a blend of meta (means virtual transcendence) and verse (a backformation from the universe). There are four categories of metaverse according to the Acceleration Studies Foundation (ASF), which is a non-for-profit technology research organization: (1) a perfect virtual story in a virtual world, (2) a mirror world resembling the real world at present, (3) an augmented reality that demonstrates a combination of augmented information in life and the real world, and (4) capturing and storing daily information about things and people. The increased number of users and activities using new technologies has generated huge amount of data in the metaverse. As the amount of data increases in the metaverse, the value, security, and reliability of the data have become a key concern too. Blockchain technology offers solutions to guarantee the reliability of the metaverse data, whereas AI keeps the rich and diverse metaverse content secure.

Blockchain and AI complement each other in the creation of the virtual world. Humans have desires and urges for creation, and therefore humans have been creating new cultures. Oh and Youn [15] described the new SeaCircle concept of culture aka human cultural activities for creating. The theory identifies creativity as one of the elements of open mind and spirit. The metaverse can be described as a platform that enables people to become more engaged in creative pursuits by resettling the resources and space limits. Recently, the real world and the virtual world have further converged due to the Fifth Industrial Revolution. This phenomenon is happening as humans and things become hyperconnected. Production and consumption are inseparable for digital Design It Yourself (DIY) and social customization. The human (offline) world makes its own effort to focus and own the fundamental 20% due to scarce resources while applying the Pareto's Law. Conversely, in the online world of information, sharing and searching opportunities from the relegated 80% of customers would be appropriate to explain the Long Tail Theory. This convergence is ubiquitous across many sectors in our everyday lives, including finance, food, healthcare, logistics, manufacturing, and sports. One example of the applications in metaverse is where multiple users can freely trade products based on the transaction method and currency via community-based platforms. Virtual assets such as Decentraland MANA and Sand in the SandBox, which were launched in 2017 and 2020, respectively, are community-driven platforms. Creators can monetize gaming experiences and voxel ASSETS using blockchain technology. The metaverse creates an alternate world that would not be possibly attained in the real world. Blockchain becomes one of the trusted technologies, so the real thing is becoming data in the virtual world.

Blockchain was first known to the world in a paper on Bitcoin: P2P Electronic Money System proposed by Satoshi Nakamoto. It is a blockchain to create and connect blocks containing data and to reach a consensus among participating modes. Algorithms such as Proof of Stake (PoS) and Proof of Work (PoW) are used in this process. Blockchain 2.0 enabled Ethereum smart contract execution with online legal effect without an intermediary. In addition, Blockchain 3.0 focuses on improving transaction processing speed and consensus algorithms and its application in expanded fields, where the synergy of blockchain and AI is reified more tangibly in the metaverse environment. For example, Decentraland allows users to buy land in a virtual real estate using MANA, an ERC-20 token. Land ownership and other collectible items are ERC-721 non-exchangeable tokens. Users can earn income by placing billboards to buildings, freely place buildings on land purchased from Decentraland, or open exhibitions by accumulating rare digital content.

This phenomenon of cognitive and scientific revolution has enabled humans to enter the phase of connected and combined intelligence with machines. The blockchain and AI technology are speeding up this phenomenon. Blockchain permits reliable and safe transactions through decentralization and now serves as a digital asset for the society. AI is at a phase where creation and prediction are achievable with pattern recognition and study using mass volume of data. When AI and blockchain technology were combined, both have changed conventional business models and have positively transformed the communities. However, one of the weaknesses of AI is its inherent centralized data storage, making it an easy target for manipulation, hacking, and data tampering. Blockchain complements AI to address its challenges. The blockchain mechanisms offer origin and immutability as well as control address privacy issues and enhance accountability of trust and decisions. A tangible outcome of combining blockchain and AI is enabling trusted digital evaluation and decision-making on mass volumes of data. It also creates an environment that secures data sharing and makes AI understandable while incorporating trust among devices. Despite this, the blockchain technology has its shortcomings. The transaction speed is slowed down when a new block is added to the blockchain. This becomes less efficient for sectors that need high speed because consensus of all nodes is needed. Due to the irreversibility of blockchain, correction for an error or vulnerability spotted in the script of smart contracts becomes an impediment. The integrity of the blockchain data can be compromised due to these vulnerabilities. Hacking millions of dollars' worth of cryptocurrencies would be disastrous. This blockchain imperfect algorithm somehow is subdued and compensated by AI's machine learning systems that enhance the security of blockchain applications. AI can aid in dynamic setting with what parameters to increase scalability, offer governance procedures, and make customization effective. In the case of public blockchain, privacy infringement is possible as any person can investigate the transaction ledgers, and it is costly to manage personal data in the blockchain. AI does not perform analysis, not without prior permission, but it is able to perform analysis on a local device belonging to the individual. AI offers personalized services to users that do not violate privacy of personal biodata. Therefore, blockchain and AI complement each other's weaknesses to make people's lives better [16]. For instance, many companies are powered by the pair of blockchain technology and AI in healthcare record sharing (BurstIQ, Gainfy), food supply chain logistics (Bext360), financial security (AI BlockChain), and media royalties (Blackbird.AI, BoxSpring Media) [16].

The phenomenon of combining the values of the blockchain and AI has made progress in recent years. Both technologies offer enhanced trust in data integrity (authenticity), a new level of intelligence to blockchain-based business networks (augmentation), and business process efficiency (automation) [17]. Automation and trust in the data for loan processing in the financial service industry allow faster closing of loan applications that enhances customer satisfaction. Healthcare organizations can better identify patient data patterns on blockchain, while AI surfaces treatment insights, promoting patient care while protecting privacy of the electronic health records. The duo in the life sciences and pharmaceutical industry add traceability and visibility to the drug supply chain and acutely improve the success rate of clinical trials. This is possible as blockchain and AI permit transparency, data integrity, automation of trial participation, consent management, patient tracking, and data collection by combining advanced data analysis within a decentralized framework. Blockchain and AI are transforming the supply chain of various sectors through digitalization and paperless process. It makes the data trustworthy for sharing and allows automation and adding intelligence to fulfill transactions. A firm can increase its decarbonization efforts by monitoring the carbon emission data of parts and products accurately to achieve a sustainable business model.

In the metaverse, various and large amounts of secondary and tertiary data are produced because of the high user activities. In the blockchain-based metaverse, this data is traceable due to its unique identification tag, and it becomes a good material for AI in the metaverse. Metaverse enables the pair of blockchain technology and AI to create a digital virtual world where users can freely and safely partake in socioeconomic activities that are beyond the real-world limits. The application of these advanced technologies is accelerated and has found its role expanding in the form of mobile payment applications in the world of metaverse.

2.3 Mobile Payment Applications

Cao et al. [18] cited that the number of users participating in mobile payment has increased exponentially. This is possible with the coordination of banking systems with the mobile payment applications. Based on Insider Intelligence [19], mobile phone users of ages 14 and above, 87.3 percent of China's smartphone users have made at least one proximity mobile payment transaction in the past 6 months, followed by South Korea (45.6%), the United States (43.2%), India (40.1%), and Japan (34.9%). Samsung Payments, Apple Payments, and Google Android Payments are extending their international payment methods, including the largest global mobile payment market players, such as WeChat and Ali Pay from China. The newly minted emerging middle-class societies largely in the two most populated countries in the world, China and India, are more conscious of the mobile payment options, and their lifestyles have improved significantly. Networld Media Group, LLC [20], found that mobile payment was the most frequently used point-of-sale payment method worldwide, accounting for 21.5% of the transaction payment market share in 2020. The boom is likely spurred by the COVID-19 pandemic where customers fear of the potential virus transmission due to handling of the paper banknotes. The mobile payment trend has seen an increase in the number of customers from about 900 million to 1.48 billion during the pandemic timeframe. It is projected to account for 33.4% of the worldwide point-of-sale transactions by 2024.

Mobile payment permits customers to do transaction and payment with mobile devices such as tablets and smartphones. Through payment instructions to financial companies and banks, customers can make fund transfers and monetary payments through mobile devices, near-field communication (NFC), and mobile plan. Financial institutions and application providers can fulfill financial services through Internet by enabling terminal devices and mobile payments for funds. Mobile payments using transportation tickets, credit cards, and membership cards via a mobile terminal convert the mobile phone into a digital wallet. Mobile terminals can free customers from travel and reduce geographical barriers of business locations. The connection between the Internet and mobile communication terminals has made it possible for round-the-clock uninterrupted financial services. Mobile payments are speedy, all-weather service, and multi-functional, and there is no need to prepare for a small change. Micropayments are payments of small amounts of less than USD10, and macropayments are about several dozens of USD via the Internet, e.g., purchases such as video downloads, drinks, and small house fixtures. Presumably under satisfying security conditions, this requires less data transmission, storage, and management for network efficiency and speed. The primary difference is that it would be adequate to use the SIM card to authenticate micropayments through the mobile network itself. On the other hand, the authentication needs to be run through a financial institution for macropayments.

Mobile phone applications are applications developed to operate on a tablet, smartphone, and other mobile devices that can be downloaded from mobile software app stores for a small fee or even for free. Mobile payment apps such as Apple Pay, Google Wallet, and Samsung Pay are creating a new trend, be it technology sophistication or business model ideation. Therefore, a business model can be designed by combining apps with mobile payment that characterizes collaboration among information communication technology, finance, and retailers based on the FinTech development [21].

Literature on mobile banking, mobile banking apps, and mobile devices has seen a remarkable progress in the emerging technologies arena. One of the more advanced sectors that experienced more tangible innovation and advancement in this arena is the banking industry and its mobile banking apps. Modern smartphones have changed the messaging between banks and individuals, and further recognizing the omnipresent penetration of mobile phones in electronic dealings would transform the methods of doing business [22]. The mission is for people to make purchases anytime and anywhere through their mobile phones. Banks, customers, and other financial service providers get to access a worldwide computing payment system. Tijani and Ilugbemi [23] claimed that Internet moveable banking helps bridge time and geographical obstacles through a range of electronic services, as customers can perform monetary transaction while on the move. It is which people initiate, pay bills, and transfer funds via electronic means using their mobile devices. Consumers with moveable devices have spurred the activation of moveable banking apps by banks in the developing and advanced economies. The total payment value reached $503 billion in 2020, 79% of smartphone owners have made an online purchase with their device in the last 6 months, and the total number of unique mobile users globally is projected to reach 5.22 billion by the end of 2021 [24]. The elderly, children, and physically challenged individuals are demanding for more location-based services, and economies of scale have made smartphones with Internet applications affordable, forging more inclusive societies. This consumer behavior and trend of using mobile devices and mobile banking apps have its own share of privacy and security issues. This may be linked to peoples' concerns about the new service platforms as most customers do not have confidence for the service channels [23]. It is when customers trust the interface and connections that channel their cash can they accept new innovations in the way that the sector demands. Security doubts and risks are what most customers have less faith in, such as not completing transactions, the challenges to retrieve or track non-completed transactions, and the time-consuming process that may take weeks or months for banks to solve the problems. Spajić [24] stated that the number of fraudulent transactions related to mobile apps has increased by 600% since 2015 (i.e., one in every 20 fraud attacks is linked to a rogue mobile app). About 89% of the digital fraud losses are associated with account takeovers that resulted in $40 million in losses. This explains why the diffusion rate and adoption level of new platforms for some banks have been slow in the developing economies. Unlike conventional payment modes, payments using the moveable devices are susceptible to hacking and bot attacks. Fraudsters use social media to advertise their virtual stores over the mobile apps and sell stolen data. Mobile banking usage figures have found some users even share their account details via email and text messages with the apparently "legitimate organizations" on social media platforms. For the less-developed African nations, which are less equipped with infrastructure, cost may represent a hindrance involving Internet subscriptions and fees related to the mobile banking apps. Extant studies have investigated the factors influencing mobile banking growth by mostly applying traditional statistical modeling, such as Pearson's correlation, partial least squares, and structural equation modeling [25–27]. Nourani et al. [28] found that the results of these models are inaccurate and unreliable, and sometimes bias, compared with the AI-based techniques that are flexible, robust, and accurate. Thus, the AI-based techniques are appropriate for research that is complex in nature, for instance, studying attitudes, behaviors, and emotions. Based on the cited strengths in Sect. 2.2, the pair of blockchain and AI primarily complements and strengthens data reliability, privacy and security including for mobile payment applications. Therefore, it is interesting to investigate these effects on personalized recommendation systems. At this point, we coined the fortified combination of blockchain with AI elements and mobile payment applications as blockchain-based mobile phone applications (BMPAs).

2.4 Personalized Recommendation Systems

BMPAs enable personalized recommendation systems that need to be appealing to its users to motivate them to make purchases over their mobile phones. Understanding the customers' purchasing behavior is of interest to businesses that apply BMPAs to share contents and recommend merchandises for users. Customers tend to be exposed with mass amount of information sources, which are irrelevant, subjecting customers to information overload. Modarresi [29] explained that this issue of information overload can be addressed with personalized recommendation systems. It is a high-level business intelligence platform that applies mass data mining to equip e-commerce sites with comprehensive personalized decision support and information services for their customers [30]. The recommendation system for shopping in websites aids customers in their purchase decisions. By recommending the product which customers are seeking for, the recommendation system automatically fulfills the process of personalized selection of products to meet the customized needs of its customers. The primary algorithms for e-commerce recommendation system encompasses collaborative filtering [31], content-based recommendations [32], and association rule-based recommendations [33]. Personalized recommendation systems enabled BMPAs to benefit business merchants as it collects user data, intelligently offers personalized recommendations to the online users, and accounts for their preferences and interests [34]. Since then, there is a proliferation of social networks and online multi *planetary* platforms that offer personalized services and gain support from referral systems [35]. In a growing competitive environment, personalized recommendation systems can attract and retain customers as these systems allow improved e-commerce services to its users [36]. Gao et al. [37] added that a recommendation system helps business merchants understand their customer behavior which benefits their marketing planning strategies. This is possible as BMPAs use the recommendation systems to create value through precise data mining analysis and findings.

2.5 Shopping Motivation Using BMPAs

Until now, there has been no concrete or unified explanation of what motivates customers to shop using BMPAs. To understand the drivers and risks behind this emerging consumerism, it would be helpful for businesses to identify specific customer's needs and wants that are associated with consumption preferences [38].

Drivers refer to the factors that attract customers to enter the online or mobile marketplace using BMPAs to fulfill their internal needs [39]. Risks would be primarily shopping risks [40] and other perceived risks [41] for online shopping. Therefore, observing shopping motivations via BMPAs assumes a pivotal role in recognizing customers' needs and meeting those needs as much as possible. In this chapter, online shopping motivation (drivers and risks) was conceptualized as the *effort that motivates or inhibits a person in his or her willingness to use the BMPA services while fulfilling one's needs and want*s. There has been a growing number of studies associated with retailing in virtual environments. Exploratory studies have intensified over the last two decades, drawing advantages such as opportunities and affordability, as well as challenges for online retailers in using the metaverse for dispensing real-world products through blockchain-based applications [42]. There are other studies that have attempted to assess the potential value of virtual trade and retailing for real companies to succeed in the electronic marketplace [43]. Beyond that, it is the virtual heterotopia that extends the *consensual hallucination* that pre-dates the commercial inception of the worldwide web by nearly a decade [44]. Various studies have investigated consumers' intention to use smartphones for mobile shopping [45], personal characteristics, consumption values, and behavioral intentions in adopting mobile shopping [46–49]. Others include motivation, loyalty, and process [50, 51], exploring the fit of real company products in the second life or virtual world [52], information that consumers look for when shopping online for groceries [53], conveniences and risks of Internet shopping behavior [54], and metaverse-retail service quality [55].

In these studies, researchers have examined the benefits of Internet or online shopping in retail and have developed guidelines when setting up virtual stores. Some studies have explored the range of factors to improve the user experience when shopping in the virtual environment. Nevertheless, limited research has been conducted to study the consumer motivation of using BMPA services. While researchers argue the main role and possible motives in their studies, a research framework to guide the study of consumer behavior using BMPAs has been sparse. Despite the broad consensus that motivation has a robust influence on consumer behavior, it is a lacuna in the literature to examine the adoption of BMPAs. This chapter attempts to understand consumer motivation, trust, adoption of BMPAs, and repeat usage of BMPAs. To achieve this, it is necessary to comprehend better the values and risks using BMPAs when performing online shopping. This would be performed through three lenses: the means-end chain theory, social identity theory, and prospect theory to discover what makes the BMPA community lives better off.

2.6 Means-End Chain Theory

Customers habitually do not consciously think about the motives underpinning their consumption behavior; thus, researchers are faced with challenges to discover these motives. A widely accepted theory to study motives is the means-end chain theory.

This section attempts to relate the means-end chain theory and to connect customer value to customer behavior. The means-end chain is applied as the core research framework presented in Sect. 2.12 in this chapter and as the method to unravel the associations between customers' cognitive hierarchical value structures [56]. This method describes how a person cognitively behaves through a consumption process hierarchically [57]. The primary principle of this method is that customers would weigh the attributes of products that will offer them to realize their personal values [56, 58]. There are three hierarchical levels of cognitive abstraction in the means-end chain theory. They are attributes, consequences, and values ([59–61]. The theory postulates that consumer behavior is driven by values which eventually influence customers' purchasing choices [62]. Gutman [60] claims that customers learn to ponder their decisions when purchasing products or services based on the physical attributes. The means (physical attributes) are fundamental to fulfill customers' wants and ends (values). Bagozzi et al. [63] further explain that benefits can become substitutes for the desired purchasing behavior due to the positive feelings formed from consuming the products and services. Xu et al. [64] argue that the means-end chain theory supports the notion that customers take actions to avoid and reduce undesired consequences. They learn what actions that they may take to produce the desired outcomes. Therefore, the desired outcomes, i.e., benefits and values, guide the consumer choice behavior [59–61].

Consumer behavior is primarily goal oriented. According to Gutman [60], the means-end chain theory is a hierarchy of goals in which higher-order goals express a deeper level of consumer motivation. In contrast, benefits are the subgoals that are secondary to values, and values can be measured as the ultimate goals that motivate consumers to display certain shopping behaviors. The means-end chain theory is an appropriate theoretical lens for differentiating lower-level goals (benefits) and higher-level goals (values) [65].

A primary postulation of the means-end chain theory is to explain that customers gain their values (ends) due to the positive benefits ensuing from the product or service attributes [59–61]. It explains that customers use products and services to enjoy benefits and values, not for the attributes per se. Henceforth, it is rational to conceptualize the benefit-value-behavior model to study the effects on BMPA identification and repeat customers' usage. Scholars theorize that value which is a superior goal may normalize customer actions that include their usage patterns and loyalty in relational company-customer exchanges [66]. Several scholars have established the linkage between value and repeat usage or purchase intention (e.g., [66, 67]). Other researchers suggest the theory on reasoned action infers that human behavior is fundamentally driven by behavioral intention [68]. Therefore, the relationships between benefit, value, identification, and repeat usage are used as the basis to develop the research framework of this study.

2.7 Social Identity Theory

The interactionist social psychology theory was originally introduced in the 1970s and 1980s to account for the nature of social groups and the group processes [69]. Social identity theory focuses on the role of self-conception which is related to the cognitive processes and social beliefs in intergroup relations and contends that individuals logically organize themselves into social categories [69]. The research on social identity theory has evolved since the 1980s. A range of sub-theories that have developed from the social identity theory focuses on self-enhancement, marginalization, nonconformity, risk reduction, motivation within groups, and leadership between and within groups [69]. The theory has also been applied to explain the phenomena involving organizations and their stakeholders [69]. In social identity, when individuals turn to be substitutable components of a shared group identity, depersonalization of the self and the rest is attained [70], which then engenders the social identity phenomenon [71].

The antecedents of social identification represent factors that cause a group's identity to be attractive to persons. For example, the uniqueness of the group characteristics from those of equivalent groups, prestige, and values are uphold by specified members [69, 71]. Through motives of uncertainty reduction, individuals consider categories that offer self-enhancement. The significance of these identifications includes behavioral and affective dimensions [72]. A few studies have differentiated identification from other organizational behavior concepts such as internalization, involvement, and commitment claiming that these may be consequences rather than components of identification itself [72, 73]. Customers can be identified with the organization and its applications. This is applicable to the BMPA environment because of the unique traits valued by its customers (identity attractiveness). The facets of the company's identity attractiveness are mostly communicated to the customers through press releases, direct marketing, personal selling, and sales promotions. Although a customer views a company's identity as prestigious and unique, the customer may not identify with the identity of the company and its applications. The trustworthiness of the company's applications affects the attractiveness of a company's identity to customers [7, 8, 66]. If a customer trusts the image of the company, the customer will potentially identify and use its product applications that are communicated to them. Identification leads customers to care and feel psychologically attached to the company which eventually results in repeat purchase intention/usage and customer loyalty. Henceforth, it is crucial to examine the relationships between values, trust, identification, and repeat usage in the adoption of BMPA.

2.8 Prospect Theory

Mobile phone applications using the blockchain technology has leapfrog during the recent years. This phenomenon marks a large customer search effort for application stores amidst fierce competition and poor utilization rates for both the developers (host companies) and their participating retailers [74]. Host companies have resorted to bundle their product applications to increase customer loyalty and to sustain a good stream of revenue for their participating retailers. However, using mobile phone applications for shopping is deemed uncertain and risky; thus customers may not always be rational [74, 75]. One related field of research that offers some basis for these ostensibly non-rational behaviors is the prospect theory. This theory has been broadly used to explain the consumer behavior under risk from the maximizing revenue standpoint [76, 77]. Prospect theory claims that individuals behave based on their assessment of the available options and their assessment rests on their level of risk aversion and outcomes [76, 77]. They compute the probabilities of outcomes that are coded as losses or gains in their current situation and then sum up a value for each option. They usually decide to follow the option that gives them the highest value [76, 77]. Customers who identify the company's applications that give them the highest value influence the attractiveness of a company's identity to customers and, in turn, their purchase decisions [7, 8, 66]. Therefore, prospect theory can be applied for modeling customer outcomes by assessing the losses and gains while shopping in the BMPA environment. Prospect theory is also found to be a suitable theoretical lens in explaining the role of perceived risk that moderates BMPA identification on repeat customer usage.

2.9 Utilitarian Value, Hedonic Value, and BMPA Identification

To investigate the relationship between the customer perceptions of BMPA shopping value and customer outcomes, it is important to comprehend the concept of value and its accompanying dimensions. Extant research has gathered that value is merely an exchange between price and quality. There are claims that value is more complex and that consumer behavior is the outcome of multi-dimensions of consumer value [78]. Utilitarian value and hedonic value are the most universal [79]. In this section, these value dimensions will be examined specifically for a BMPA shopping context.

Utilitarian value is described as a judgment of functional benefits and costs [80]. And it is pertinent for task-specific use of BMPA for shopping. These include considering product offerings, monetary savings, and convenience during the pre-purchase stage [79, 81]. This accentuates the need to further separate utilitarian value as something different from hedonic value; also, utilitarian value concerns the cognitive components of attitude, such as convenience, value for money, and product variety in the BMPA context [79, 81]. This section solicits that shoppers may shop using the BMPAs because of the convenience of locating and comparing retailers and conserving the psychological and temporal resources [79, 81].

On the other hand, hedonic value is described as an overall evaluation of experiential benefits and costs, such as adventure and gratification [81]. Hedonic value dimensions have been posited as a subject of much discussion in the mobile phone shopping literature [79, 81]. Researchers have started to recognize other online shopping elements such as the application's role, best deals gained, social implications, and shopping ideas [82]. In this discursive chapter, the aim is to examine if all these elements are transferable to the BMPA context. Like offline and online shopping, BMPA shoppers also shop for the off-the-beaten track experiences and entertainment reasons that absorb the users and let them break free from their routines [83].

Customers may respond favorably to the utilitarian value and hedonic value derived from using BMPA as a more attractive shopping environment compared to the conventional offline and online shopping. This strengthens the identity communicated through the BMPA. A BMPA offers companies with the platform to foster a specific image that customers may perceive as upholding and parallel to their social and personal definition. Therefore, the following hypotheses have been developed:

H_1: Utilitarian value is positively related to BMPA identification.
H_2: Hedonic value is positively related to BMPA identification.

2.10 BMPA Trustworthiness, BMPA Identification, and Repeat Customers' BMPA Usage

The trustworthiness of an identity influences the customers' attractiveness to a company and its applications. Customers are more likely to identify with the company's applications if they trust the image portrayed through the company's media channels [7, 8, 66]. Identification leads to customers' growing concern for the company which results to customers' resistance to negative information while forging repeat customers' usage and customer loyalty [7, 8, 66]. On the other hand, customer-company identification can lead to non-supportive behaviors [84] such as negative word of mouth about the company and imposing unrealistic demands from the company. This attraction toward a particular BMPA can be enhanced through ongoing communications with the customers that forge a degree of trustworthiness for the perceived BMPA identity. The development of the BMPA identification ensues when the BMPA becomes a salient choice for customers when making their forthcoming purchase decisions. It is assumed that customers who possess some knowledge of the company's identity are participants of the company's loyalty program. These customers have formed a strong identification with the BMPA through many communications and transactions beforehand [85].

Nevertheless, BMPA identification is unlike the dimensions generally found in customer purchase intention studies such as brand equity [86], customer commitment [87], customer loyalty [88], and customer satisfaction [89]. The dimensions are the consequences of a customer's cognitive process of self-categorizing within the perceived identity forged by BMPAs. Through a customer's self-categorization process, the BMPA identification then manifests into behaviors such as repeat customer usage or customer loyalty. These behaviors are formed due to market-related factors such as high market entry barriers, superior products, and excellent business models. Even so that this competitive edge declines, the BMPA identification lingers since customers find their sense of social categorization and self-definition by identifying themselves with the company's BMPAs. In short, repeat customer usage may result from the BMPA identification. Henceforth, it is imperative for companies to nurture a clear identity for BMPA because it sustains a competitive edge in an increasingly competitive market.

H_3: BMPA trustworthiness is positively related to BMPA identification.
H_4: BMPA identification is positively related to repeat customers' BMPA usage.

2.11 Perceived Risk

Shopping preludes risk. This is because a customer's purchase decision has results that cannot be faultlessly prophesied, and some of which possibly become unpleasant [76, 77]. Shopping risk is more noticeable in company mobile phone applications than in the conventional brick-and-mortar shopping due to spatial-temporal separation between the companies and customers [40]. Past literature establishes that perceived risk is a determinant for initial usage and repeat usage intention [41]. In this chapter, the perceived financial risk is defined using the Cunningham [90] scale that infers the likelihood of monetary loss due to maintenance costs, hidden costs, or a lack of warranty. To better reflect the BMPA context, the perceived risk is extended to encompass performance risk, i.e., the potential loss due to failing in meeting the product quality expectations, the payment app function fails to work when shopping, and when a participating retailer refuses to accept payment using the BMPA e-payment functions, as well as privacy risk, i.e., the probability of losing control over personal information.

Higher shopping risk potentially shifts the customers' focus from getting hold of the item to the shopping experience. Take gambling for example, individuals entertain the risk of monetary loss for the states of high arousal during the timings of ambiguity, as well as the positive arousal resulting from the winnings [91, 92]. Similarly, customers view shopping using BMPA to be riskier than the brick-and-mortar shopping. However, these customers usually determine if the risks are within their tolerable limits before they are willing to shop using the BMPA. They will use the BMPA if it fulfills their needs to experience fun, gratification, novelty, and other complex sensations while accepting the potential risks that they could face [91, 92].

Therefore, the influence of BMPA identification on repeat customers' BMPA usage will decrease as a function of perceived risk.

H_5: Perceived risk negatively moderates the relationship between BMPA identification and repeat customers' BMPA usage.

2.12 Control Variables and the Research Model

The customer outcome framework for blockchain-based mobile phone applications (BMPAs) in Fig. 1 holds onto the customers' perceived value which is defined as a trade-off between benefits and costs. It evaluates utilitarian value and hedonic value as the benefits gained which is identified with a BMPA. Additionally, the trustworthiness that customers place on BMPAs is assessed to reflect how much customers want to identify themselves with the BMPA. On the other hand, perceived risk becomes the major cost of shopping using BMPA and is modelled as a moderator in Fig. 1. Overall, this framework implies that customers would assess value and trustworthiness identified with the BMPAs and weigh the risks when forming their intention. The means-end theory connects customer value and customer behavior [59–61], while the social identity theory suggests customers potentially identify with a company and trust its applications because of the unique traits valued by its customers (identity attractiveness) [69, 71]. The prospect theory claims that individuals behave by computing the probabilities of outcomes (losses and gains) and decide to follow the option that offers them the highest value [76, 77].

The Customer Outcome Framework is a path diagram. The ellipses in the path diagram represent the latent constructs while the rectangles symbolize the observed variables ([93], p. 11; [94], p. 2). The latent constructs in Fig. 1 are the utilitarian value, hedonic value, and BMPA trustworthiness. They are the second-order constructs in the framework. The utilitarian value is measured by three subconstructs, namely, product offerings [95, 96], monetary savings [97], and BMPA convenience [48]. The hedonic value is measured indirectly by six subconstructs, which are adventure, gratification, role, best deal, social, and idea [98]. Meanwhile the BMPA trustworthiness is measured by three subconstructs, namely, the benevolence, competence, and integrity [99–101]. The scale measurements of the BMPA identification are adapted from Bhattachrya and Sen's [102] study and the repeat customers' BMPA usage from Suh and Han's [103] research work; both are observed variables. Perceived risk is measured by items relating to financial loss, failure to meet product quality expectations, embarrassment, non-acceptance by participating retailers to use BMPA payment functions, and loss of control over personal information [104, 105].

There are three control variables specified in Fig. 1 to manage the likely spurious effects in the research model. The first is the number of past transactions that a customer have made using a BMPA to purchase products and paid using its

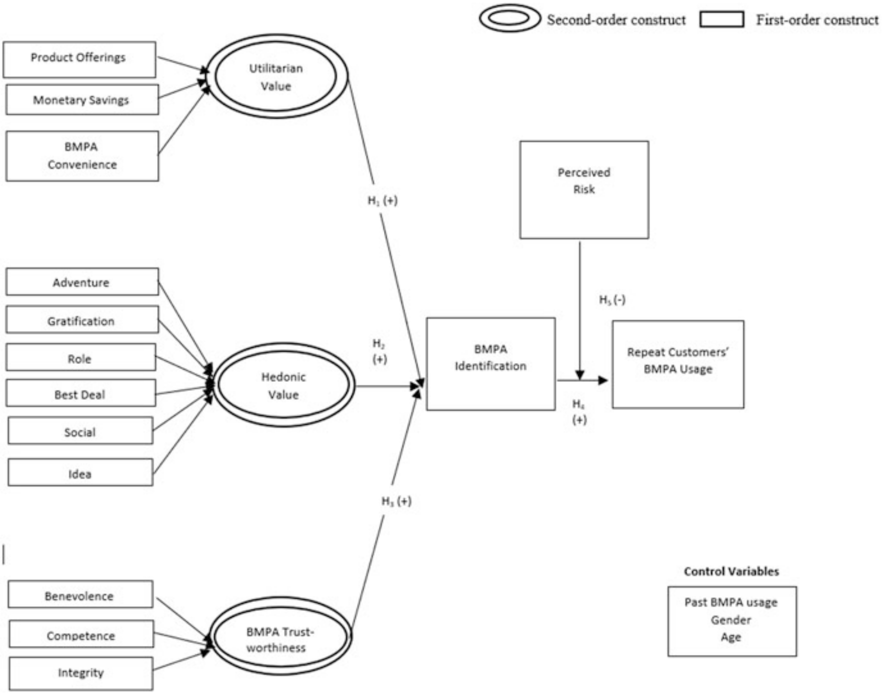


Fig. 1 Customer outcome framework for blockchain-based mobile phone applications (BMPAs)

digital wallet. The other two are gender and age to ensure good representation of male/female shoppers and different age groups to reduce bias and to improve data accuracy. Singapore would be a suitable test bed for data collection due to the high penetration of BMPA usage and the growing number of companies recognizing the increased competition in the electronic marketplace.

The Customer Outcome Framework depicts three positive impacts of utilitarian value, hedonic value, and BMPA trustworthiness on the BMPA identification. H_1, H_2, and H_3 infer when a customer perceived a higher utilitarian value, hedonic value, and BMPA trustworthiness; it would increase the BMPA identification and in turn customers' repeat BMPA usage (H_4). However, when customers perceived risk is high, it influences customers' BMPA identification and consequently reduces their repeat BMPA usage (H_5). Pertaining to the degree of impact for the five constructs on the repeat customers' BMPA usage, future researchers may gather empirical evidence to test the five hypotheses in the framework.

The model may be tested with the structural equation modelling (SEM) using AMOS (Analysis of Moments Structures) software. SEM is found useful for gathering empirical data that is designed to confirm a research study design rather than to explore or explain a phenomenon [106]. SEM is capable in examining multivariate causal relationships in ecological studies [107] such as the framework in Fig. 1. Other than the direct effects, SEM can study the indirect effects on pre-assumed causal relationships [107] such as the moderating effects of perceived risk on BMPA identification and the repeat customers' BMPA usage**.** Although SEM is the mostly applied technique for path modelling, researchers have taken more interest in using the partial least square (PLS) [108]. PLS possesses several advantages over SEM [108]. PLS has a built-in capability to cope with formative indicators and test moderating relationships with a small sample size [108]. Yildiz [109] evaluates PLS-SEM bias at a relatively large sample size (560 consumers) in the mobile shopping context, but the bias does not seem to diminish when estimating data from common factor populations. This has put forward the recommendation to apply SEM or PLS technique, whenever it is more appropriate based on the sample size and the study of the indirect effects on pre-assumed causal relationships.

3 Discussions

3.1 Theoretical Implications

The literature review presented in this chapter claims that there is continuing progress in retail-related publications in terms of studying relevancy of value and risk dimensions in offline and online shopping environment. Nevertheless, the literature review also showed that there is lacuna in the electronic business context and research domains. The proposed Customer Outcome Framework signifies the cross-disciplinary research between computer science (the upstream research) and social science in studying consumer behavior (the downstream research).

This chapter answers the call for more research effort in studying the BMPA adoption in businesses. A continuous stream of conceptual work that will apply critical perspectives to the BMPA adoption phenomenon is a great need for research related to the value, trustworthiness, and risk tolerance of the end users. Thus, these three important concepts, i.e., value, trustworthiness, and risk, need to be defined specifically. This is to establish a win-win relationship between the company and its customers who use BMPAs in their business ecosystems. From the academic point of view, subsequent empirical studies and findings in Singapore's electronic payment market would contribute significant value to the existing mobile banking industry and to the retailing literature.

3.2 Practical Implications

The findings of this chapter enable the stakeholders in the businesses to be better prepared in optimizing results by investing in the BMPA technology that benefit their customers. A few practical implications can be derived from the discussions in this chapter. Firstly, this chapter reveals the application of BMPAs across various sectors. As such, this chapter stimulates interested practitioners to think about the huge potential service innovations through BMPAs beyond the end consumer offerings such as in the climate control measures, business sustainability, cybercrime, e-sports, real estate, e-learning, and logistics. Secondly, there is still lack of research about customers' perceptions, behaviors, and impacts on continued customer patronage and impacts on companies, such as organizational restructuring, reskilling, and jobs redesigning to prepare for improving yield from the e-commerce businesses using BMPAs. Explicit identification of motivations (the drivers and perceived risk) patterns would inform retailers by proposing effective marketing strategies for different market segments. The built-in AI elements in BMPAs and the derived data patterns can improve marketing strategies as they can be linked closely to the customer motivation for online business transaction. Retailers can assess the marketing strategies by monitoring the motivation fulfillment before market launching. Comprehending customers' expectations will offer retailers' insights into what customers wanting to obtain and satisfy when using the BMPAs. By personalizing the offerings that links to these primary motivations, retailers can meet and satisfy customers' demands. Thirdly, the interrelationships shown in Fig. 1 in this chapter identify broadly the versatility in which different sectors would find BMPAs useful. The Customer Outcome Framework denotes that more work is needed of computer science engineers in two primary ways: firstly, whether they can bundle industry offerings while offering adventure, gratification, best deals, convenience, and fulfilling the customers' social needs through their development of BMPA algorithms and software features, and secondly, BMPAs that are developed on the blockchain and AI technologies that can be programmed to meet the goals for profit and not-for-profit sectors that concerns people's well-being. For the betterment of people's lives, be it the government, companies, and individuals, BMPAs can be further unlearned, relearned, and fortified to serve the larger communities including environment management and social inclusion other than economic contribution. The objective is that this leads to the triple bottom-line gains and embracing towards the 2030 Agenda that is to protect prosperity, people, planet, peace, and partnership.

3.3 Limitation

The literature review was based mostly on the English indexed publications from the two largest databases with scientific publications (ABDC publications, Scorpus), one largest archive website (Researchgate.net), and an academic search engine (Google Scholar). It is important to note that there are relevant articles that are not incorporated in other e-library databases and there are only a few conference proceedings referred in this chapter. Future research might focus on reviewing publications in other languages and databases as well.

4 Conclusions and Future Research

In the recent years, blockchain-based mobile phone applications (BMPAs) have been growing rapidly. BMPAs have become an opportunity for businesses to increase their selling of products and to forge customer loyalty. The discussion in this chapter conceptualizes a research framework for the businesses in the BMPA environment applying three theories, namely, the means-end chain theory, the social identity theory, and the prospect theory. It is gathered that Singapore would be a suitable test bed for future data collection since it has a sizeable electronic payment community and there is a high penetration rate of BMPA usage in this island city. A critical review of relevant literature from 1991 to 2021 has been carried out. This chapter visited topics on how the duo of the blockchain technology and AI has fortified the BMPAs that enable trust, security, and convenience for its users. It is a win-win exchange as businesses gain to learn more of customers' preferences due to the data mining which AI can offer. The blockchain technology and AI complement each other weaknesses in the application of BMPA. The literature review revealed that the different variables discussed in this chapter have varying impact on repeat customers' BMPA usage. Past studies signified that an increase in perceived hedonic value, utilitarian value, and trustworthiness influence a company's identification. A favorable company's identification can lead to an increase in repeat customers' usage. Therefore, similar study of the relationship between these constructs in the BMPA context is timely.

Empirical research on the chapter advocating Customer Outcome Framework in the BMPA environment will be necessary in the proposed Singapore electronic payment market. While this conceptual stage of Customer Outcome Framework is deemed appropriate as the first stage for scoping to obtain insights of the BMPA field, there is no empirical study on it so far. Thus, future studies may perform qualitative, quantitative, mixed methods, and longitudinal studies to further investigate the motivations for BMPA repeat customer usage. Additionally, scholars could investigate other mediator variables of BMPA shopping such as the level of user friendliness and the ease of navigating the app features. There is still a lack of research on studying the owners-managers and staff perceptions that require their active participation in research and their willingness to disclose their business strategies, business performance measures against industry benchmarks. Other stakeholders such as telecommunication companies, bank officials, government regulatory bodies, and Internet services providers could be considered in future works to study the adoption of BMPA in the entire business ecosystem. Mobile phone applications are ever more becoming part of community lives, and individuals' attitudes toward these BMPAs affect their frequency of usage and, in turn, the value derived from using these applications over their mobile devices. A/B testing and experiments could be performed to assess the value obtained for non-, ex-, first-time- and regular BMPA shoppers. Hidden costs could include nomophobia that can impact one's mental health due to mobile device obsession. Oniomania that is compulsive buying behavior or shopping addition is another. Significant harm to an individual's life is that when he or she is always preoccupied on their mobile devices and neglects other life (job and family) commitments. Other potential costs include digital eye strain over prolonged hours of using the BMPAs, potential accidents due to loss of concentration because users are glued to their mobile devices, and even experience loss of sense of time. Some may experience withdrawal symptoms when their mobile devices are unreachable including restlessness, irritability, tension, anger, and depression. Proposed studies should examine other factors from moral, ethical principles, and society's fairness as Singapore is a melting pot which predominantly consists of Chinese, Malay, Indian, and others (Sinhalese, Buginese, Sikhs, Peranakans, Eurasians, *Orang Laut* – seaman in Malay). Examining across cultures in different ethnic groups should be a strategic direction for future research efforts to confront and to obtain a more in-depth understanding of the topic. Future research could involve across different generation cohorts (Baby Boomers, Generation X, Y, and Z). This connection varies among individuals and regions across the world. Henceforth, the Customer Outcome Framework can be adapted in other countries to gather further insights. Finally, studies that are examining and measuring the 3Ps (people, profit, and planet) and their direct and indirect impacts of BMPA on macro (destination), meso (industry) and micro (company) levels are recommended.

References

1. T. Dogru, M. Modi, C. Leonardi, Blockchain technology and its implications for the hospitality industry (2018). www.bu.edu/bhr. Retrieved May, 2019
2. J.W. Overby, E.-J. Lee, The effects of utilitarian and hedonic online shopping value on consumer preference and intentions. J. Bus. Res. **59**(10–11), 1160–1166 (2006)
3. K. Ryu, H. Han, S. Jang, Relationships among hedonic and utilitarian values, satisfaction and behavioral intentions in the fast-casual restaurant industry. Int. J. Contemp. Hosp. Manag. **22**(3), 416–432 (2010)
4. B.B. Dedeoglu, A. Bilgihan, B.H. Ye, P. Buonincontri, F. Okumus, The impact of servicescape on hedonic value and behavioral intentions: the importance of previous experience. Int. J. Hosp. Manag. **72**, 10–20 (2018)
5. X. Zheng, J. Men, F. Yang, X. Gong, Understanding impulse buying in mobile commerce: an investigation into hedonic and utilitarian browsing. Int. J. Inf. Manag. **48**, 151–160 (2019)
6. H.W. Kim, S. Gupta, A comparison of purchase decision calculus between potential and repeat customers of an online store. Decis. Support Syst. **47**, 477–487 (2009)
7. J. Chen, C. Zhang, Y. Xu, The role of mutual trust in building members' loyalty to a C2C platform provider. Int. J. Electron. Commer. **14**(1), 147–171 (2009)
8. X. Cheng, Y. Gu, J. Shen, An integrated view of particularized trust in social commerce: an empirical investigation. Int. J. Inf. Manag. **45**, 1–12 (2019)
9. Monetary Authority of Singapore (MAS), E-payments (2021). https://www.mas.gov.sg/development/e-payments. Retrieved November, 2021
10. N. Choy, Digital wallets to overtake credit cards by 2024 amid e-commerce boom: Report. https://www.straitstimes.com/business/banking/digital-wallets-to-overtake-credit-cards-by-2024-amid-e-commerce-boom-report. Retrieved November, 2021

11. Monetary of Authority Singapore (MAS), Reply to Parliamentary Question on e-payments and progress on the roll out of SGQR (2021, October 4). https://www.mas.gov.sg/news/parliamentary-replies/2021/reply-to-parliamentary-question-on-e-payments-and-progress-on-the-roll-out-of-sgqr. Retrieved November, 2021
12. Infocomm Media Development Authority (IMDA), Half of Singapore's hawkers now offering e-payments (2021, February 19). https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2021/Half-of-Singapores-Hawkers-Now-Offering-E-payments. Retrieved November, 2021
13. Visa Inc., Digital payments and online shopping on the rise among seniors in Singapore: Visa Study (2019). https://www.visa.com.sg/about-visa/newsroom/press-releases/digital-payments-and-online-shopping-on-the-rise-among-seniors-in-singapore-visa-study.html. Retrieved November, 2021
14. H.-J. Jeon, H.-C. Youn, S.-M. Ko, T.-H. Kim, Blockchain and AI meet in the metaverse (2021, June 28). https://www.intechopen.com/online-first/77823. Retrieved November, 2021
15. J.-S. Oh, H.-C. Youn, A study of new concept of culture, in *Proceedings of the Korea Contents Association Conference*, Seoul (2004), pp. 54–60
16. S. Daley, Tastier coffee, hurricane prediction and fighting the opioid crisis: 31 ways blockchain & AI make a powerful pair (2020, April 6). https://builtin.com/artificial-intelligence/blockchain-ai-examples. Retrieved November, 2021
17. IBM, Blockchain and artificial intelligence (AI) (2021). https://www.ibm.com/topics/blockchain-ai. Retrieved January, 2022
18. X. Cao, L. Yu, Z. Liu, M. Gong, L. Adeel, Understanding mobile payment users' continuance intention: a trust transfer perspective. Internet Res. **28**(3), 456–476 (2018)
19. Insider Intelligence. Proximity mobile payment user share in select countries (2021). https://www.emarketer.com/chart/248566/proximity-mobile-payment-user-share-select-countries-2021-of-smartphone-users. Retrieved November, 2021
20. Networld Media Group, LLC, Mobile wallet use growing worldwide, reveals data report. https://www.retailcustomerexperience.com/news/mobile-wallet-use-growing-worldwide-reveals-data-report/. Retrieved November, 2021
21. A. Karim, V. Chang, A. Firdaus, Android botnets: a proof-of-concept using hybrid analysis approach. J. Organ. End User Comput. **32**(3), 52–67 (2020)
22. S.K. Sharma, M. Sharma, Examining the role of trust and quality dimensions in the actual usage of mobile banking services: an empirical investigation. Int. J. Inf. Manag. **44**, 65–75 (2019)
23. J. Tijani, A. Ilugbemi, Electronic payment channels in the Nigeria banking sector and its impacts on national development. Asian Econ. Financ. Rev. **5**, 521–531 (2015)
24. D.J. Spajić, Mobile banking statistics that show wallets are a thing of the past (2021, March 17). https://dataprot.net/statistics/mobile-banking-statistics/. Retrieved November, 2021
25. A.A. Shaikh, R. Glavee-Geo, H. Karjaluoto, How relevant are risk perceptions, effort, and performance expectancy in mobile banking adoption? Int. J. E-Bus Res. **14**(2), 39–60 (2018)
26. N. Urbach, F. Ahlemann, Structural equation modeling in information systems research using partial least squares. J. Inf. Technol. Theor. Appl. **11**, 5–40 (2010). https://aisel.aisnet.org/jitta/vol11/iss2/2. Retrieved March, 2021
27. S. Rahi, M.A. Ghani, A structural equation modeling (SEM-AMOS) for investigating brand loyalty and customer's intention towards adoption of internet banking, in *Proceedings of the 29th International Scientific Conference on Economic and Social Development*, Rabat (2018, May 10–11), pp. 206–220. https://www.esd-conference.com/conference/30. Retrieved December, 2018
28. V. Nourani, H. Gökçekus, I.K. Umar, Artificial intelligence-based ensemble model for prediction of vehicular traffic noise. Environ. Res. **180**(1–4), 108852 (2020)
29. K. Modarresi, Recommendation system based on complete personalization. Procedia Comput. Sci. **80**(4), 2190–2204 (2016)
30. W. Xu, J. Sun, J. Ma, W. Du, W., A personalized information recommendation system for R&D project opportunity finding in big data contexts. J. Netw. Comput. Appl. **59**(3), 362–369 (2016)

31. J. Xiao, M. Wang, B. Jiang, A personalized recommendation system with combinational algorithm for online learning. J. Ambient Intell. Humaniz. Comput. **9**(6), 667–677 (2018a)
32. X. Zheng, Y. Luo, L. Sun, X. Ding, J. Zhang, A novel social network hybrid recommender system based on hypergraph topologic structure. World Wide Web (Bussum) **21**(4), 985–1013 (2018)
33. F.F. Santos, M.A. Domingues, C.V. Sundermann, V.O. Carvalho, S.O. Rezende, Latent association rule cluster-based model to extract topics for classification and recommendation applications. Expert Syst. Appl. **112**(1), 34–60 (2018)
34. M. Gorgoglione, U. Panniello, A. Tuzhilin, Recommendation strategies in personalization applications. Inf. Manag. **56**(6) (2019). https://doi.org/10.1016/j.im.2019.01.005. Retrieved November, 2021
35. A. Corbellini, C. Mateos, D. Godoy, A. Zunino, S. Schiaffino, An architecture and platform for developing distributed recommendation algorithms on large-scale social networks. J. Inf. Sci. **41**(5), 686–704 (2015)
36. H. Hwangbo, Y.S. Kim, K.J. Cha, Recommendation system development for fashion retail e-commerce. Electron. Commer. Res. Appl. **28**(1), 94–101 (2018)
37. M. Gao, B. Ling, L. Yang, J. Wen, Q. Xiong, S. Li, From similarity perspective: a robust collaborative filtering approach for service recommendations. Front. Comp. Sci. **13**(2), 231–246 (2018)
38. J.N. Sheth, B.I. Newman, B.L. Gross, Why we buy what we buy: a theory of consumption values. J. Bus. Res. **22**(2), 159–170 (1991)
39. W.J.K. Jih, S.F. Lee, An exploratory analysis of relationships between cellular phone uses' shopping motivators and lifestyle indicators. J. Comput. Inf. Syst. **44**(2), 65–73 (2004)
40. Y. Li, L. Yang, H. Shen, Z. Wu, Modeling intra-destination travel behavior of tourists through spatio-temporal analysis. J. Destin. Mark. Manag. **11**, 260–269 (2019)
41. P.K. Chopdar, V.J. Sivakumar, Understanding continuance usage of mobile shopping applications in India: the role of espoused cultural values and perceived risk. Behav. Inf. Technol. **38**(1), 42–64 (2019)
42. A.I. Sanka, M. Irfan, I. Huang, R.C. Cheung, A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research. Comput. Commun. **169**, 179–201 (2021)
43. L.H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, P. Hui, *From Internet and Extended Reality to Metaverse: Technology Survey, Ecosystem, and Future Directions* (Cornell University, 2021). https://arxiv.org/pdf/2110.05352.pdf. Retrieved November, 2021
44. D. van der Merwe, The metaverse as virtual heterotopia, in *3rd World Conference on Research in Social Sciences*, Vienna (2021, October 22–24). https://www.dpublication.com/wp-content/uploads/2021/10/41-20250.pdf. Retrieved November, 2021
45. S. Agrebi, J. Jallais, Explain the intention to use smartphones for mobile shopping. J. Retail. Consum. Serv. **22**(1), 16–23 (2015)
46. K. Bin Dost, M. Illyas, C. Abdul Rehman, Online shopping trends and its effects on consumer buying behavior: a case study of young generation of Pakistan. NG-J. Soc. Dev. **5**(1), 1–22 (2015)
47. R. Assarut, S. Eiamkanchanalai, Consumption values, personal characteristics and behavioral intentions in mobile shopping adoption. Market-Tržište **27**(1), 21–41 (2015)
48. T.L. Childers, C.L. Carr, J. Peck, S. Carson, Hedonic and utilitarian motivations for online retail shopping behavior. J. Retail. **77**(4), 511–535 (2001)
49. P. Duarte, S.C.E. Silva, M.B. Ferreira, How convenient is it? Delivering online shopping convenience to enhance customer satisfaction and encourage e-WOM. J. Retail. Consum. Serv. **44**(5), 161–169 (2018)
50. B. Barnard, D. Menoe, Online shopping: motivation, loyalty and process. Expert J. Mark. **8**(1), 48–72 (2020)
51. G. Christodoulides, N. Michaelidou, Shopping motives as antecedents of e-satisfaction and e-loyalty. J. Mark. Manag. **27**(1–2), 181–197 (2010)

52. S.J. Barnes, J. Mattsson, Exploring the fit of real brands in the second life 1 virtual world. J. Mark. Manag. **27**(9–10), 934–958 (2011)
53. Y. Benn, T.L. Webb, B.P. Chang, J. Reidy, What information do consumers consider, and how do they look for it, when shopping for groceries online? Appetite **89**(6), 265–273 (2015)
54. A. Bhatnagar, S. Misra, H.R. Rao, On risk, convenience, and internet shopping behavior. Commun. ACM **43**(11), 98–105 (2000)
55. E. Gadalla, K. Keeling, I. Abosag, Metaverse-retail service quality: a future framework for retail service quality in the 3D internet. J. Mark. Manag. **29**(13–14), 1493–1517 (2013)
56. J. Gutman, A means-end chain model based on consumer categorization processes. J. Mark. **46**(2), 60–72 (1982)
57. V.A. Zeithaml, Consumer perceptions of price, quality, and value: a means-end model and synthesis of evidence. J. Mark. **52**(3), 2–22 (1988)
58. R. Barrena, T. García, M. Sánchez, Analysis of personal and cultural values as key determinants of novel food acceptance, application to an ethnic product. Appetite **87**(4), 205–214 (2015)
59. C.F. Lin, Advertising effect evaluation based on means-end chain theory, in *Ideas in Marketing: Finding the New and Polishing the Old*, (Springer, Cham, 2015), p. 353
60. J. Gutman, Means–end chains as goal hierarchies. Psychol. Mark. **14**(6), 545–560 (1997)
61. R. Nunkoo, H. Ramkissoon, Applying the means-end chain theory and the laddering technique to the study of host attitudes to tourism. J. Sustain. Tour. **17**(3), 337–355 (2009)
62. I. Rahman, D. Reynolds, The influence of values and attitudes on green consumer behavior: a conceptual model of green hotel patronage. Int. J. Hosp. Tour. Adm. **20**(1), 47–74 (2019)
63. R.P. Bagozzi, D. Belanche, L.V. Casaló, C. Flavián, The role of anticipated emotions in purchase intentions. Psychol. Mark. **33**(8), 629–645 (2016)
64. X. Xu, F.K. Chang, E.Y. Li, Exploring consumer value path of cross-border e-commerce: a perspective of means-end theory, in *ICEB 2018 Proceedings*, vol. 75, Guilin (2018), pp. 284–294
65. L. Xiao, Z. Guo, J. D'Ambra, Benefit-based O2O commerce segmentation: a means-end chain approach. Electron. Commer. Res. **19**(2), 409–449 (2018b)
66. J.C.Y. Chai, N.K. Malhotra, F. Alpert, A two-dimensional model of trust–value–loyalty in service relationships. J. Retail. Consum. Serv. **26**, 23–31 (2015)
67. C. Gan, W. Wang, The influence of perceived value on purchase intention in social commerce context. Internet Res. **27**(4), 772–785 (2017)
68. G. Brodowsky, K. Stewart, B. Anderson, Brand and country influences on purchase intentions: a theory-of-reasoned action approach. J. Promot. Manag. **24**(2), 251–269 (2018)
69. M.A. Hogg, Social identity theory, in *Understanding Peace and Conflict Through Social Identity Theory*, (Springer, Cham, 2016), pp. 3–17
70. M. Fujita, P. Harrigan, G.N. Soutar, Capturing and co-creating student experiences in social media: a social identity theory perspective. J. Mark. Theory Pract. **26**(1–2), 55–71 (2018)
71. A.D. Brown, Identities in organization studies. Organ. Stud. **40**(1), 7–22 (2019)
72. T.C. Guo, X. Li, Positive relationship between individuality and social identity in virtual communities: self-categorization and social identification as distinct forms of social identity. Cyberpsychol. Behav. Soc. Netw. **19**(11), 680–685 (2016)
73. R.A. Rather, L.D. Hollebeek, Exploring and validating social identification and social exchange-based drivers of hospitality customer loyalty. Int. J. Contemp. Hosp. Manag. **31**(2), 1432–1451 (2019)
74. J. Wan, L. Zhao, Y. Lu, S. Gupta, Evaluating app bundling strategy for selling mobile apps: an ambivalent perspective. Inf. Technol. People **30**(1), 2–23 (2017)
75. Y. Yang, Y. Liu, H. Li, B. Yu, Understanding perceived risks in mobile payment acceptance. Ind. Manag. Data Syst. **115**(2), 253–269 (2015)
76. A. Tversky, D. Kahneman, Advances in prospect theory: cumulative representation of uncertainty. J. Risk. Uncertain. **5**(4), 297–323 (1992)
77. D. Kahneman, A. Tversky, Prospect theory: an analysis of decision under risk, in *Handbook of the Fundamentals of Financial Decision Making: Part I*, (World Scientific Publishing, Hackensack, 2013), pp. 99–127

78. M.G. Gallarza, M.E. Ruiz-Molina, I. Gil-Saura, Stretching the value-satisfaction-loyalty chain by adding value dimensions and cognitive and affective satisfactions: a causal model for retailing. Manag. Decis. **54**(4), 981–1003 (2016)
79. A.B. Ozturk, K. Nusair, F. Okumus, N. Hua, The role of utilitarian and hedonic values on users' continued usage intention in a mobile hotel booking environment. Int. J. Hosp. Manag. **57**, 106–115 (2016)
80. J. Park, S. Ha, Co-creation of service recovery: utilitarian and hedonic value and post-recovery responses. J. Retail. Consum. Serv. **28**, 310–316 (2016)
81. C.J. Parker, H. Wang, Examining hedonic and utilitarian motivations for m-commerce fashion retail app engagement. J. Fash. Mark. Manag. **20**(4), 487–506 (2016)
82. K.F. Hashim, M. Yusof, S. Affendi, R. Ahmad, The influence of hedonic values on s-commerce adoption behavior. Adv. Sci. Lett. **21**(5), 1561–1565 (2015)
83. M.H. Yrjölä, H. Kuusela, E. Närvänen, T. Rintamäki, H. Saarijärvi, Leading change: a customer value framework, in *Leading Change in a Complex World: Transdisciplinary Perspectives*, (Tampere University Press, Tampere, 2019), pp. 145–163
84. M.S. Balaji, S.K. Roy, S. Sadeque, Antecedents and consequences of university brand identification. J. Bus. Res. **69**(8), 3023–3032 (2016)
85. J. Kang, T.B. Alejandro, M.D. Groza, Customer–company identification and the effectiveness of loyalty programs. J. Bus. Res. **68**(2), 464–471 (2015)
86. S.L. Lee, Y. Namkung, H.H. Yoon, A study on the effect of customer equity on behavioral intentions: moderating effect of restaurant type. Culin. Sci. Hosp. Res. **24**(2), 51–62 (2018)
87. E. Anastasiadou, C. Lindh, T. Vasse, Are consumers international? A study of CSR, cross-border shopping, commitment and purchase intent among online consumers. J. Glob. Mark. **32**(4), 239–254 (2018)
88. A.M.R. Karimi, A. Esmaeili, A. Sepahvand, V. Davidaviciene, The effect of customer equity drivers on word-of-mouth behavior with mediating role of customer loyalty and purchase intention. Eng. Econ. **29**(2), 236–246 (2018)
89. G.T.M. Hult, P.N. Sharma, F.V. Morgeson III, Y. Zhang, Antecedents and consequences of customer satisfaction: do they differ across online and offline purchases? J. Retail. **95**(1), 10–23 (2019)
90. S.M. Cunningham, The major dimensions of perceived risk, in *Risk Taking and Information Handling in Consumer Behavior*, ed. by D. F. Cox, (Harvard Business Process, Boston, 1967), pp. 82–264
91. C. Bonnaire, C. Bungener, I. Varescon, Pathological gambling and sensation seeking–how do gamblers playing games of chance in cafés differ from those who bet on horses at the racetrack? Addict. Res. Theory **14**(6), 619–629 (2006)
92. K.B. Mercer, J.D. Eastwood, Is boredom associated with problem gambling behaviour? It depends on what you mean by 'boredom'. Int. Gambl. Stud. **10**(1), 91–104 (2010)
93. J.L. Arbuckle, IBM SPSS Amos 22 User's Guide (2013). https://www.sussex.ac.uk/its/pdfs/SPSS_Amos_User_Guide_22.pdf. Retrieved January, 2022
94. Z. Awang, *SEM Made Simple: A Gentle Approach to Learning Structural Equation Modeling* (MPWS Rich Publication, Bangi, 2015)
95. D.M. Szymanski, R.T. Hise, E-satisfaction: an initial examination. J. Retail. **76**(3), 309–322 (2000)
96. Y. Bakos, The emerging role of electronic marketplaces on the internet. Commun. ACM **41**(2), 35–42 (1998)
97. T. Rintamäki, A. Kanto, H. Kuusela, M.T. Spence, Decomposing the value of department store shopping into utilitarian, hedonic and social dimensions: evidence from Finland. Int. J. Retail. Distrib. Manag. **34**(1), 6–24 (2006). https://doi.org/10.1108/09590550610642792. Retrieved January, 2022
98. M.J. Arnold, K.E. Reynolds, Hedonic shopping motivations. J. Retail. **79**(2), 77–95 (2003)
99. D. Gefen, Customer loyalty in e-commerce. J. Assoc. Inf. Syst. **3**(1), 27–51 (2002)
100. D.H. McKnight, V. Choudhury, C. Kacmar, C., Developing and validating trust measures for e-commerce: an integrative typology. Inf. Syst. Res. **13**(3), 334–359 (2002)

101. W. Wang, I. Benbasat, Recommendation agents for electronic commerce: effects of explanation facilities on trusting beliefs. J. Manag. Inf. Syst. **23**(4), 217–246 (2007)
102. C.B. Bhattacharya, S. Sen, Consumer-company identification: a framework for understanding consumers' relationships with companies. J. Mark. **67**, 76–88 (2003)
103. B. Suh, I. Han, The impact of customer trust and perception of security control on the acceptance of electronic commerce. Int. J. Electron. Commer. **7**(3), 135–161 (2003)
104. M.S. Featherman, P.A. Pavlou, Predicting e-services adoption: a perceived risk facets perspective. Int. J. Human-Comp. Studies. **59**(4), 451–474 (2003)
105. G. Pires, J. Stanton, A. Eckford, Influences on the perceived risk of purchasing online. J. Consum. Behav. **4**(2), 118–131 (2004)
106. G. Devault, Structural Equation Modeling (SEM) (2018, September 12). https://www.thebalancesmb.com/quantitative-research-using-structural-equation-modeling-2297146. Retrieved January, 2022
107. Y. Fan, J. Chen, G. Shirkey, Applications of structural equation modeling (SEM) in ecological studies: an updated review. Ecol. Process. **5** (2016). https://doi.org/10.1186/s13717-016-0063-3. Retrieved January, 2022
108. J.D. Shackman, The use of partial least squares path modeling and generalized structured component analysis in international business research: a literature review. Int. J. Manag. **30**(3), 78–85 (2013)
109. O. Yıldız, PLS-SEM bias: traditional vs consistent. Qual. Quant., 1–16 (2022). https://doi.org/10.1007/s11135-021-01289-2. Retrieved January, 2022

Part III
Blockchains and Healthcare

A Secure Decentralized Privacy-Preserving Healthcare System Using Blockchain

Aderonke Thompson, Hafiz Odekunle, and Boniface Alese

1 Introduction

Healthcare is a concentrated knowledge space in which vast quantities of information are processed, accessed, and distributed all the time [2]. Storing and sharing a massive number of records is necessary and challenging due to the sensitivity of health information and others that restrict data, regarding security and privacy. In the healthcare field, knowledge exchange is vitally essential for diagnosis and decision making. Information exchange is vital for medical professionals to be able to communicate with each other and pass patient information to the competent authority for other purposes, such as testing. The exchange of medical information must be achieved across a safe network and must also ensure that the privacy of patients is maintained.

Healthcare blockchain is an innovation that helps to safely customize stable health data, share it by blending the complete real-time information of a patient's health, and store it as a secured healthcare arrangement [5]. This technology permits transactions by participants in dispersed, permanent, straightforward, secure, and auditory ways, which allow access to records from the first transaction, which can be confirmed and examined by any entity. The chain is continually developing and new blocks holding references, that is, a hash value is being added to the existing block [3]. Blockchain is structured as a peer-to-peer (P2P) network that links with numerous network nodes. All the nodes in the system have a public key and a private key for securing information exchange. Blockchain transaction uses a public key for encryption to guarantee consistency, irreversible, and non-reputability of records while decryption of the message uses the private key for integrity and verification of

A. Thompson (✉) · H. Odekunle · B. Alese
Federal University of Technology, Akure, Nigeria
e-mail: afthompson@futa.edu.ng; bkalese@futa.edu.ng

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_9

every transaction made by node [5]. In this regard, only the public key and private key authentic messages go to the network for affirmation [1]. The challenge of the technique is that solitary clients with a particular private key are permitted to sign the transaction. Also, mistakes during transmission of the information lead to system failure, for example, confirming an advanced signature. The transactions that are considered legitimate are broadcasted in the network domain by the miners. The miners decide data transactions to admit in the distributed public ledger based on the chosen consensus protocol used, for examples proof-of-work (PoW) and proof-of-stake (PoS). The approval nodes check that the communicated block encompasses large transactions and references the former block in the chain utilizing the matching hash value. Thus, attaining these requirements implies that the new blocks are added to the blockchain; otherwise, it drops the block.

2 Overview and Related Work

There are different types of blockchains based on the managed data, on the accessibility of such data, and on what operation can be performed by the user. These include public permissionless, consortium (public permission), and private.

Public permissionless: This is a state-of-the-art public blockchain protocols based on proof-of-work (PoW) consensus algorithms with open source and not permission. Anyone can participate as a node or miner without permission. All data in the blockchain is accessible and visible to everyone, although parts of the blockchain can be encrypted to secure data and preserve user's anonymity. Examples are Bitcoin, Ethereum, or Litecoin.

Consortium (public permissioned): This type of blockchain operates under the leadership of a group. As opposed to public blockchain, they do not allow any person with access to the Internet to participate in the process of verifying transactions; only a selected group of nodes can participate in the distributed consensus process. It is used within one or across many institutions. When a consortium blockchain is created within one institution (e.g., financial sector), it is initiated for restricted public use and fractionally centralized. On the other hand, a consortium between institutions (e.g., insurance companies, financial institutions, governmental institutions) is unlocked for public use while still having created a relatively centralized trust.

Private: In a private blockchain, write permissions are kept centralized to one trusted organization, while read permissions may be public or restricted. A private blockchain only allows selected nodes to connect to the network. It is, therefore, yet a distributed centralized network. Private blockchains control which nodes can perform transactions, execute smart contracts, or act as miners. It is used for private purposes. Hyperledger Fabric and Ripple are examples of blockchain platforms that only support private blockchain networks. Table 1 presents the summary of the types of blockchain.

Table 1 Difference between public, consortium, and private blockchain

	Public	Consortium	Private
Participants	Permissioned Identified Trusted	Permissioned Identified Trusted	Permissioned Identified Trusted
Consensus Mechanisms	Proof of Work, Proof of Stake, etc. Large energy consumption. No finality 51% attack	Voting or multi-party consensus algorithm Lighter Faster Low energy consumption Enable finality	Voting or multi-party consensus algorithm Lighter Faster Low energy consumption Enable finality
Access	Open Read/Write	Permissioned Read and /or Write	Permissioned Read and /or Write
Transaction Approval Frequency	Long Bitcoin: 10min or more	Short	Short
Speed	Slower	Faster	Faster
Security	Proof of Work Proof of Stake Other Consensus Mechanisms	Approved participants	Approved participants

2.1 Consensus Protocols

In a world where trust is expensive, it is essential to understand the unstable nature of trust and to figure out some measures of consensus among ourselves in respect to that which we hold as "truth." For the blockchain network to continue as functional, its peers need to come to terms with a specific state of the distributed ledger and on a way for storing data into blocks. Such terms are known as a distributed consensus protocol and it affirms the chronological order of generated transactions.

2.1.1 Proof-of-Work (PoW)

PoW is carried out by miners who conducted through miners competing to solve a cryptographic problem—also known as a hash puzzle. These miners help to verify every Bitcoin transaction, where it involves producing a hash-based PoW that is based on previous transaction blocks (read up on the Merkle Tree for more information) and forms a new branch with a new transaction block. This means that the work is moderately difficult for the miners to perform but easy for the network to verify. The first miner who manages to produce the PoW is awarded some Bitcoins. Over time, the amount of Bitcoin awarded decreases.

2.1.2 Proof-of-Stake (PoS)

Unlike PoW where new transaction blocks are created based on computational work done by solving a complex cryptographic puzzle, PoS allows a forger (instead of a miner) to stake any amount of cryptocurrency held, to be probabilistically assigned a chance to be the one validating the block—the probability based on the amount of cryptocurrency staked. Additionally, for most PoS systems, instead of receiving a cryptocurrency reward (in the above case, the Bitcoin miners receives some Bitcoins for solving a PoW), the forgers instead take the transaction fees as rewards.

The idea of putting coins to be "staked" prevents bad actors from making fraudulent validations—upon false validation of transactions, the amount staked will be forfeited. Hence, this incentivizes forgers to validate legitimately. In the recent year, PoS has gained attention, with Ethereum switching towards a PoS from a PoW consensus system.

2.1.3 Delegated Proof-of-Stake (DPoS)

DPoS is similar to PoS in regard to staking but has a different and a more democratic system that is said to be fair. Like PoS, token holders stake their tokens in this consensus protocol. Instead of the probabilistic algorithm in PoS, token holders within a DPoS network are able to cast votes proportional to their stake to appoint delegates to serve on a panel of witnesses—these witnesses secure the blockchain network. In DPoS, delegates do not need to have a large stake, but they must compete to gain the most votes from users.

It provides better scalability compared to PoW and PoS as there are fully dedicated nodes who are voted to power the blockchain. Block producers can be voted in or out at any time, and hence the threat of tarnishing their reputation and loss of income plays a major role against bad actors [10]. No doubt, DPoS seems to result in a semi-centralized network, but it is traded off for scalability.

Like PoS, DPoS has also gained attention over the years with several projects adopting this consensus algorithm. Since it was invented by Dan Larimer, DPoS has been refined continuously, from BitShares to Steem and now in EOS.

2.1.4 Proof-of-Authority (PoA)

PoA is known to bear many similarities to PoS and DPoS, where only a group of preselected authorities (called validators) secure the blockchain and can produce new blocks. New blocks on the blockchain are created only when a super majority is reached by the validators. The identities of all validators are public and verifiable by any third party—resulting in the validator's public identity performing the role of proof-of-stake. As these validators' identities are at stake, the threat of their identity being ruined incentivizes them to act in the best interest of the network.

Since PoA's trust system is predetermined, concerns have been raised that there might be a centralized element with this consensus algorithm. However, it can be argued that semi-centralization could actually be appropriate within private/consortium blockchains—in exchange for improved scalability. Newer blockchain start-ups have ventured into implementing PoA. In addition, Ethereum testnets like Rinkeby and Kovan explores the use of a PoA consensus algorithm.

2.1.5 Access Control Mechanism with Smart Contract for Data Sharing

Sharing healthcare data is considered to be a critical approach to improve the quality of healthcare service and reduce medical costs. Though current EHR systems bring much convenience, many obstacles still exist in the healthcare information systems in practice, hinder secure and scalable data sharing across multiple organizations, and thus limit the development of medical decision making and research [7]. From the foregoing, there are risks of the single-point attack and data leakage in a centralized system. Besides, patients cannot preserve the ownership of their own private data to share with someone who they trust. It may result in unauthorized use of private data by curious organizations. Furthermore, different competing organizations lacking partnership trust are not willing to share data, which would also hinder the development of data sharing [9].

In this case, it is necessary to ensure security and privacy protection and return the control right of data back to users in order to encourage data sharing. It is relatively simply to deal with security and privacy issues when data reside in a single organization, but it will be challenging in the case of secure health information exchange across different domains. Meanwhile, it also needs to further consider a suitable technique to boost efficient collaboration in the medical industry.

Securing access control mechanism as one of the common approaches requires that only authorized entities can access sharing data. This mechanism includes access policy commonly consisting of access control list (ACL) associated with data owner. ACL is a list of requestors who can access data and related permissions (read, write, update) to specific data. Authorization is a function of granting permission to authenticated users in order to access the protected resources following predefined access policies. The authentication process always comes before the authorization process. Access policies of this mechanism mainly focus on who is performing which action on what data object for which purposes. Traditional access control approaches for EHRs sharing are deployed, managed, and run by third parties. Users always assume that third parties (e.g., cloud servers) perform authentication and access requests on data usage honestly. However, in fact, the server is honest but curious. It is promising that combining blockchain with access control mechanism is to build a trustworthy system. Users can realize secure self-management of their own data and keep shared data private. In this new model, patients can predefine access permissions (authorize, refuse, revoke), operation (read, write, update, delete), and duration to share their data by smart contracts on the blockchain without the loss of control right. Smart contracts can be triggered on the blockchain once all of preconditions are met and can provide audit mechanism for any request recorded in the ledger as well. There are many existing studies and applications applying smart contract for secure healthcare data sharing. A study proposed that patients can authorize access to their record only under predefined conditions (research of a certain type, and for a given time range) [15].

Smart contract placed directly on the blockchain verifies whether data requestors meet these conditions to access the specified data. If the requestor does not have the access rights, the system will abort the session. Similarly, smart contracts in a study [4] can be used for granting and revocation of access right and notifying the updated information as providers move in and out of networks.

Researchers designed a decentralized record management system based on blockchain, called MedRec [1]. In this system, patient-provider relationship contract is deployed between any two nodes in which patients manage and share medical records with healthcare providers. Providers can add or modify this record in the case of patient's permissions. Data access record is preserved in the block to track the malicious entities when violated access activities happen. They also designed a simple graphical interface tool that allows patients to share off-chain data with fine-grained access control.

The similar design is proposed in [13]. Researchers developed an access protocol based on smart contract through admin component when mobile users send the request [12]. Smart contract will verify any transaction by predefined policies of access protocol to prevent malicious attack and achieve reliable EHRs sharing. But curious miners may infer personal information during the mining process due to the processing transactions including area ID, mobile gateway ID, and patient ID. A study creatively adopted the channel scheme of Hyperledger Fabric, which separates different types of activities for users in the different channels to share different grained data [8]. Chaincode (smart contract) can be launched in the channel with different access type, permissioned operations, and selective shared data specified in the certificate by data owners. In addition to data sharing, such a channel scheme makes good use of Fabric to enhance data privacy.

2.2 Smart Contract

A smart contract is a tamper-proof computer program or protocol that can verify and execute itself. Nick Szabo comes up with the idea of smart contract in 1994. It allows executing code without the third parties. A smart contract comprises of the value, address, functions, and state. It accepts transaction as an input and triggers event as the output after executing the corresponding code. Implementation of function logic determines the state of the contract. The necessity of smart contract has been the major focus since the emergence of blockchain technology in 2008 when the technology comes into existence through Bitcoin cryptocurrency because it has the capacity to publicly maintain database and peer-to-peer transactions securely and create a trustful environment. Smart contracts are auditable and irreversible. All the transaction information is present in a smart contract, and it executes automatically. A smart contract is machine readable, an event-driven program, autonomous, and distributed.

Solidity is a high-level language used to implement smart contracts. Developing blockchain platform of solidity are Ethereum, ErisDB, Zeppelin, and Counterparty. According to Nick Szabo, the contractual clauses (collateral, bonding, delineation of property rights) should be encoded and embedded in the required hardware and software. This helps to minimize the requirement of any trusted third party for communication using smart contracts and at the same time makes the system secure against any malicious attack. In the case of blockchain-based smart contracts, contracts are nothing but scripts residing on the blockchain, which has the ability to execute them. One can trigger a transaction to a smart contract by using the unique addresses assigned to it by the blockchain technology. Let us take an example to better understand the working of smart contracts. Suppose you want to sale your house or rent your apartment to someone, then you can simply deploy a smart contract in an existing blockchain network. Information regarding the property can be stored in the blockchain and anyone belonging to that network can access that information, but they cannot change it. In this way, you can find a buyer for your property without the need of any third party. For a wide range of potential applications, blockchain-based smart contracts could offer a number of benefits:

- Speed and real-time updates
- Accuracy
- Lower execution risk
- Fewer intermediaries
- Lower cost
- New business or operational models (Fig. 1)

With the technology growing fast, human living standard also grows vastly. In the recent use of developed devices and supporting technology, human can monitor his or her health condition just sitting at home. There are lots of devices that are already developed to read different attributes in the human body. These data can be collected using low-end device and processing locally to get quick information [17]. Blockchain technology helps to maintain the privacy of the patients and maintained

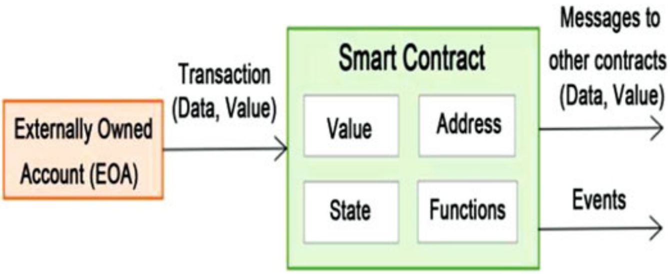

Externally Owned Account (EOA)
Transaction (Data, Value)
Smart Contract
Value
Address
State
Functions
Messages to other contracts (Data, Value)
Events

Fig. 1 Structure of smart contract

data in digital ledger format. A smart contract can be used in that system to make the system more reliable and automated. Using a smart contract, human can write some terms and conditions which could be applied once data are collected. Then it will execute these smart contracts and trigger corresponding events.

The blockchain has the capability to boost data sharing in healthcare. Researchers provide an easier way for patients to govern their medical data by developing App HGD (Healthcare Data Gateway) which is built in blockchain technology [14]. All data are managed using data management layer and stored on blockchain cloud. Patients' data are accessible solely via an authorized user; in addition, data replica may be enforced to be destroyed when the authorized time elapsed.

A study also proposed an exchange network approach for health information [15]. The two contributions are as follows: it makes use of electronic health record (EHR) semantic and design checking to organize all EHRs in the blockchain network to solve the issue of interoperability. Also, an algorithm is proposed to select the next miner randomly to reduce the power and system resources used in computation of POW. In addition, it is suggested that privacy and anonymity can be provided using blockchain encryption, smart contracts, and privacy-preserving keyword searches, but detailed approaches were not included.

Researchers proposed a medical system called MedRec which was based on smart contracts for effective and simpler administration of EHRs [2]. Registrar contracts (RCs) are used to map the user's identification string to their Ethereum addresses to keep anonymity of the users. Summary contracts (SCs) contained links that referenced patient-provider relationships (PPRs) to ensure that all the medical records of patients are connected. How patients' data are managed and accessed is defined in PPRs. However, the detailed approaches to solve an issue such as how to encrypt the patients' EHR, accessed by authorized users, user authentication, etc.

A study proposed a blockchain and MedRec-based way to deal with unravel security issues such as confidentiality, access control, privacy, audibility, and integrity in sharing healthcare data [16]. The barriers are tackled by using a signcryption and attribute-bases authentication (ABA) to ensure that process of data sharing is secure. The proposed model provides the following services: (1) Data authenticity—the validness of patients' EHRs can be confirmed by who access the information. (2) Data integrity—it ensures that stored patients' EHRs are guided against altering. (3) Data confidentiality—patients' EHRs are stored securely and stayed discreet from the unapproved user.

Researchers adopt Ethereum blockchain smart contracts to achieve efficient collaboration, data integrity, and protection of patient privacy. Protecting healthcare professional's privacy and securing links to establish an interoperability end-to-end reachable network among independent healthcare system are provided by [9]. The research solves the problem by storing the patient health records in a secure off-chain database and makes a secure socket to trade authorization-based access to tolerant information utilizing standard public key cryptography.

A study formulated a data sharing mechanism using Blockchain [9]. The mechanism was made up of three components, namely, client, control system, and storage. It is an efficient, secure identity-based authentication and key agreement protocol.

An effective security measure based on personality validation and key understanding protocol is adopted to assure user anonymity and authenticity. Keys were generated to execute client confirmation and enrollment, client verification, and request creation. A study proposes a structure that characterizes some authorization access rules through the Hyperledger Fabric [11], where a service provider can access medical record of patients in a crisis condition under the limitations of patient's permission through the system. Smart contract handled authorization and fetching of data of all transactions from ledger which makes the framework secured, efficient, and auditable.

3 Methodology

Blockchain is invented for storing financial-related records and provides a structure for actualizing a decentralized system. Each node of the blockchain interacts with another via cryptographically encrypted information exchange, and the transaction-based state system of the blockchain is known as smart contracts [6]. It was first fully implemented by Ethereum. A smart contract is client rights management tools that provide coordination and enforcement frameworks for network participant agreements without traditional legal contracts being required [7]. For instance, a smart contract characterizes the application logic that executes at whatever point an exchange happens in the trading of digital money.

Ethereum smart contracts create intelligent and logical representations of existing health data stored on each node on the network. The smart contract contains the metadata of a patient's data, access permission, and data integrity. The contract enforces that each transaction made on the blockchain system conveys a cryptographically signed information to oversee these traits. Contracts implement approaches to create data exchanges by valid blockchain transactions only and execute any set of rules consigning a specific health record; so far it can be processed.

3.1 System Design

The design integrates each node to an existing EHR system. Each node, specifically representing healthcare providers, is expected to have already databases with medical records saved on servers connected to the network.

The system design is made up of three layers, namely, data collection layer, data repository layer, and data sharing layer.

Data collection layer In this layer, electronic health records (HER) are generated by a service provider, i.e., a medical doctor. The EHRs are signed by a medical doctor using content extraction signature (CES) scheme and the signed EHRs are forwarded to the patients. Patients can extract sensitive information of EHR and create authentic extraction signature in order to avert privacy in case there is leakage during the data sharing.

Data repository layer This layer is responsible for storing the EHR and its indexes. The layer comprises of the following components:

1. *EHR manager*: This represents the different health institutions in the local system; these local systems are connected to blockchain network; the primary role of the system in our design is to store the EHRs and generate indexes that points to the stored EHR. The EHR manager consist of the following:

   (a) API library: API library will manage and control the operation of the system. The API executes a function call to interact with blockchain by parsing blockchain protocol to connect with an Ethereum client.
   (b) Ethereum client: This operates an extensive set of tasks, which include peer-to-peer network connection, encoding transactions, and transmitting transactions in addition to keeping a verified local copy of the blockchain.
   (c) Database manager: This manages access to the node's local database and ensures permission governance storage on the blockchain. The database manager checks the blockchain contracts for address verification request which is acceptable to query access. On verifying the address, the query is run on the node's local database and then results are returned to the client.

2. *Blockchain server*: This serves like a cloud server, which is responsible for saving and communicating the electronic health records (EHRs). The EHR storage location links and predefined access permission (smart contracts) of the patients are stored in the blockchain. The smart contract ensures that data are shared securely and records each access request and activities in the blockchain for the purpose of auditing in the future (Fig. 2).

Data sharing layer The authorized users (patients, healthcare providers, researchers) can initiate a request for patients' EHRs which can be granted or denied based on the predefined conditions set by the patients. Also, patient can revoke access given to a user at any given time. The logical and intelligent access control is designed using Ethereum's smart contract. The contract contains the storage link of patient's EHRs, access permission, and timestamp. The contract enforces that each transaction made on the blockchain system carries a cryptographically signed instructions to manage data integrity. The smart contract is structured as follows:

(a) Identity catalog contract (ICC): Identity catalog contract is one of the major contracts deployed on electronic health record management system (EHRMS); this contract only occurs once and invokes by every node present on EHRM network. It maps patient identity strings to their Ethereum address public key and provider IP address (Fig. 3).

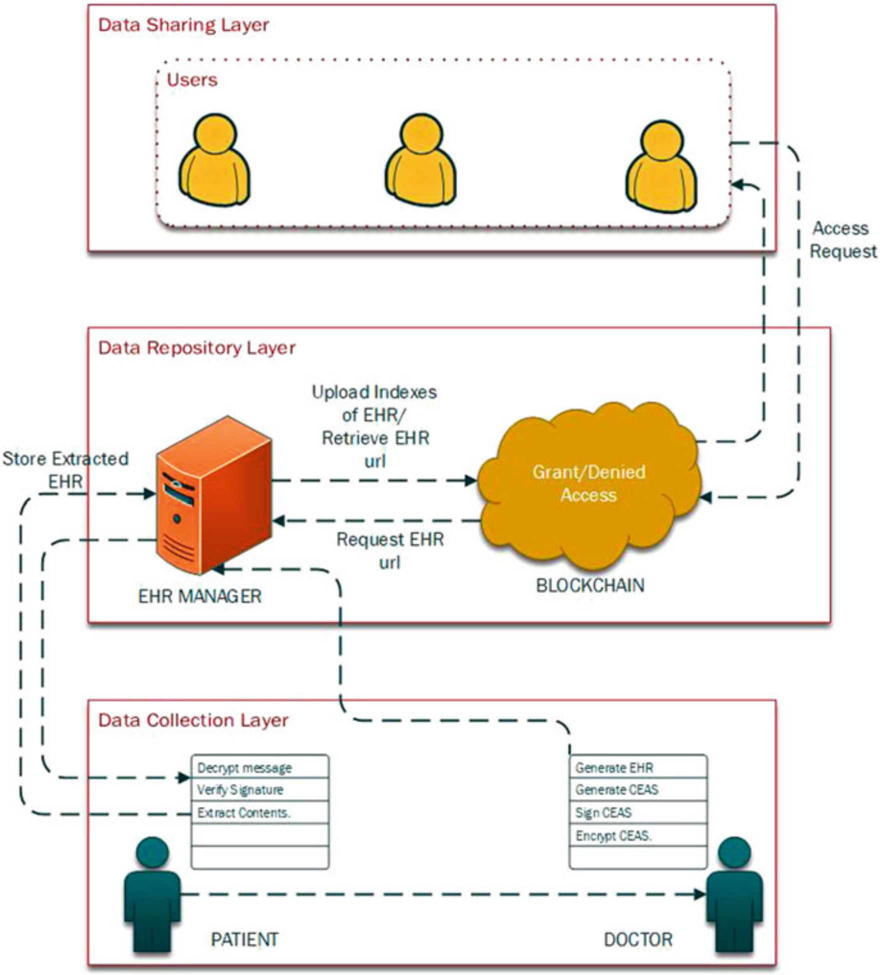


Fig. 2 Proposed system design

(b) Relationship contract (RC): The relationship contract established a patient-provider relationship (PPR) between all entities who have access to EHR of a particular patient. For each contract, one patient and provider are connected to it. The PPR is also made up of a list of unlimited third parties who are granted permission to only view the patient EHR. Patient, provider, and third-party relationships are stored on the blockchain and enable the third party to locate all providers in EHRMS network that has access to a particular patient's EHR instead of searching for them one after the other. EHRMS enables the patient to have total control over who accesses their EHR and complete audits of their EHR which are being accessed through PPR contracts.

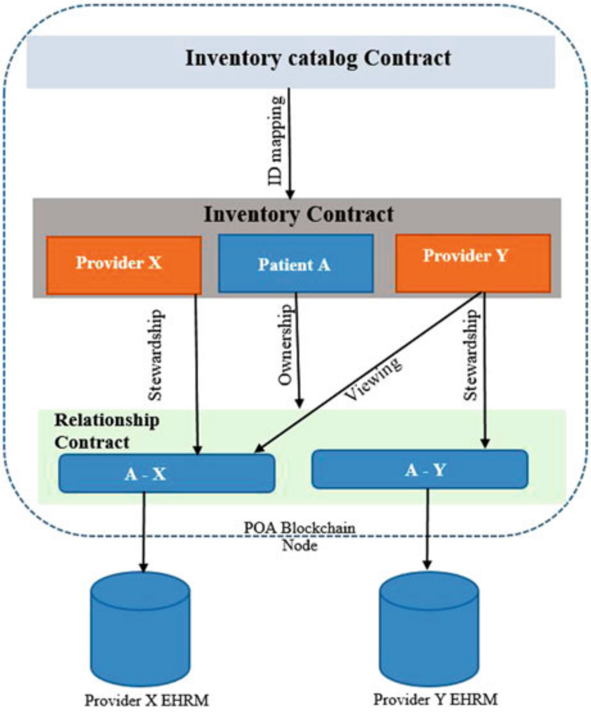


Fig. 3 Relationship graph between contract and network nodes

(c) Inventory contract (IC): IC holds a list of references to RC, representing all the participant's previous and current transactions with other nodes in the system. The contract represents actors in EHRM. Patients communicate the system by utilizing an inventory contract as a proxy. Information about entities present in the system are stored in these contracts. Information stored on the contract include patient-provider relationship (PPR) and some addresses that are associated with the individual account. These contracts require only for the patient as it serves as a pointer to all PPR that is stored in one place on the blockchain and also for easier retrieval PPR if the patient needs to recover their account using recovery secrete text.

3.2 Content Extraction Signature

In this work, document processing operation call extraction is used to remove certain selected part of the signed EHR before it is stored in the EHR manager and available for user on the blockchain network. This is done to revoke sensitive data that prevent anonymous participation of patients on the blockchain. Content extraction signature allows a patient P, the owner of EHRs which was signed by a doctor D, to extract part of EHRs and send only those parts to a user U, which helps us to assure the patient's privacy.

The content extraction signature (CES) scheme can be defined as follows: CES = (GK, Sig, Ext, Ver) which represents four algorithms, namely, key generation algorithm, signature generation algorithm, signature extraction algorithm, and signature verification algorithm.

3.2.1 Key Generation GK(k)

This algorithm chooses a security parameters k and generates a public/private key pair (pk, sk).

Pick a large prime number P and a generator g in Z_p

```
$y \leftarrow pg;$
$Q \leftarrow (p-1)(g-1);$
Select a random number q in such a way that gcd($q, Q$) = 1.
Compute:
$d \leftarrow q^{-1} mody;$
Publish Public Key $pk \leftarrow (y,q)$ and Private Key $pk \leftarrow (y,q,d)$
Algorithm 2
```

3.2.2 Signature Generation Algorithm Sig (SK, M, CEAS)

This algorithm accepts private key (sk), EHRs document (M), and a content extraction signature structure CEAS and produce content extraction signature σ_F.

```
Parse Doctor private key sk $\leftarrow$ (y, q, d); Patients EHR, M and
Content Extraction Signature Structure CEAS
$N \leftarrow Len(M);$
$T \leftarrow \{0,1\};$
For i $\epsilon [n]$
$h[i] \leftarrow H(CEAS||T||i||M_i);$
$\sigma[i] \leftarrow h[i]^d mod\ y;$
$\sigma_F \leftarrow H(CEAS||T||<\sigma[i]>_{i\epsilon[n]});$
Return $\sigma_F$
```

3.2.3 Signature Extraction Algorithm Ext(pk, M, σ_F, X)

This algorithm accepts a public key *pk*, a EHR document *M*, a Content extraction signature σ_F, an extraction subset *X*, and produce an extracted signature σ_E.

```
Parse $pk = (y,q)$
Parse $\sigma_F \leftarrow H(CEAS||T||<\sigma[i]>_{i\epsilon[n]})$
$\sigma \leftarrow \prod_{i\in X}\sigma[i]\ mod\ y$
$\sigma_E \leftarrow (CEAS, T, \sigma)$
Return $\sigma_E$
```

3.2.4 Signature Verification Algorithm $Ver(pk, M', \sigma_E)$

This algorithm accepts a public key pk, an extracted subdocument M', and an extracted signature ,σ_E, and produces a verification decision $d \in \{Acc, Rej\}$, where Acc implies "Accept" and Rej indicates "Reject."

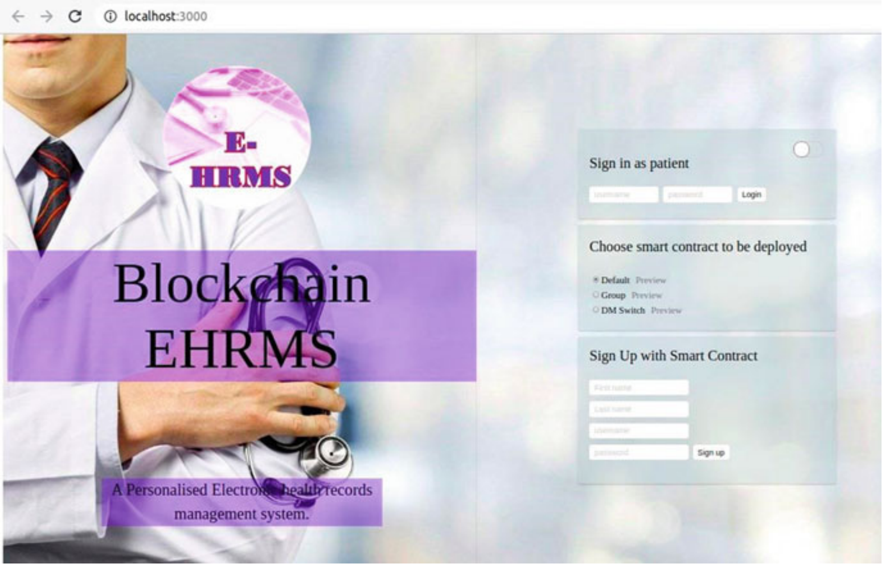
```
Parse $pk = (y,q)$
Parse $\sigma_E \leftarrow (CEAS, T, \sigma)$
Parse $M^1$
$X' \leftarrow CI(M') : n \leftarrow len(M')$
For $i \in X'$
$h[i] \leftarrow H(CEAS, T, n, i, M'[i])$
if
$\sigma^q \equiv \prod_{i \in X'} h[i] (mod\ y)$ and $X' \in CEAS$
Return Acc
Else Return Rej
```

4 Implementation

The designed system, electronic health record management system (EHRMS), works by joining three components together: (1) a front end which is a web application that allows patients/provider to access EHRMS; (2) an EHR manager that communicates with provider databases, and file system; and (3) an Ethereum blockchain that controls access rights to EHRM and connects each EHR manager to the peer-to-peer network. In summary, patients initiate access contracts that are saved on the blockchain. Therefore, the contracts determine providers' actor that should be permitted to access the EHR.

4.1 Front End

This is a component of the system that the user interacts with. All patients and service providers communicate with the system through this interface. The front end was developed using React framework. React is a JavaScript library for building a user interface with simple views for each state of the application; it communicates to the local and remote server through WebSockets. Users' private keys and other details are stored on local machines while providers use a remote server to store information of users that have a relationship with them (Figs. 4 and 5).



localhost:3000

Blockchain EHRMS

A Personalised Electronic health records management system.

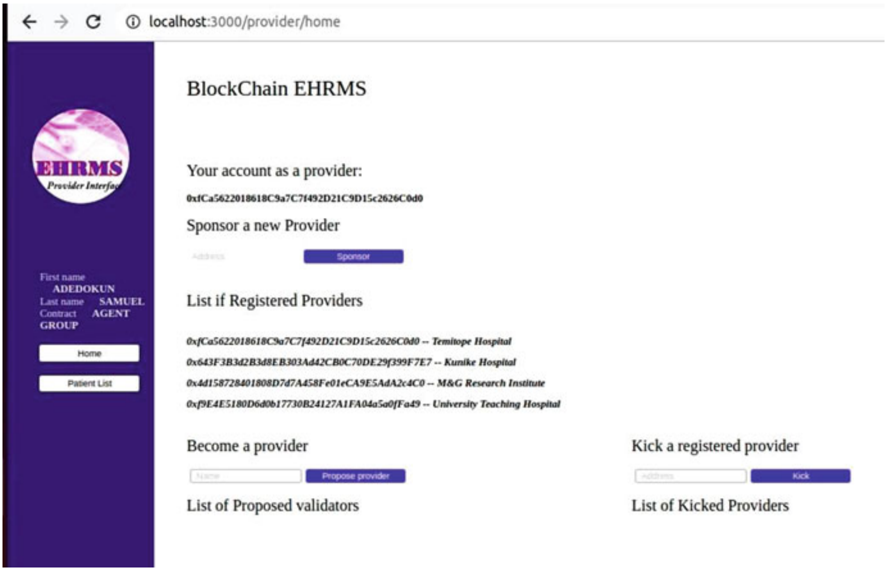
Sign in as patient

Choose smart contract to be deployed

● Default Preview
○ Group Preview
○ DM Switch Preview

Sign Up with Smart Contract

Fig. 4 EHRMS front end landing page



localhost:3000/provider/home

First name ADEDOKUN
Last name SAMUEL
Contract AGENT GROUP

BlockChain EHRMS

Your account as a provider:

0xfCa5622018618C9a7C7f492D21C9D15c2626C0d0

Sponsor a new Provider

List if Registered Providers

0xfCa5622018618C9a7C7f492D21C9D15c2626C0d0 -- Temitope Hospital
0x643F3B3d2B3d8EB303Ad42CB0C70DE29f399F7E7 -- Kunike Hospital
0x4d158728401808D7d7A458Fe01eCA9E5AdA2c4C0 -- M&G Research Institute
0xf9E4E5180D6d0b17730B24127A1FA04a5a0fFa49 -- University Teaching Hospital

Become a provider

List of Proposed validators

Kick a registered provider

List of Kicked Providers

Fig. 5 Service provider home page

4.2 EHR Manager

The EHR manager segment of EHRMS connects with the basic file system and facilitates correspondence between EHRMS hubs. It is essentially written in GoLang, albeit a few collaborations with the blockchain network require script written in JavaScript.

Remote procedure calls (RPCs) are orders given by one PC to conjure functions on another. The protocol is transport rationalist and can be applied to the Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP), WebSocket, and different protocols for sharing information over the web. EHRMS utilizes RPC in two different ways, between the users and a local database, and between the users and a remote provider database.

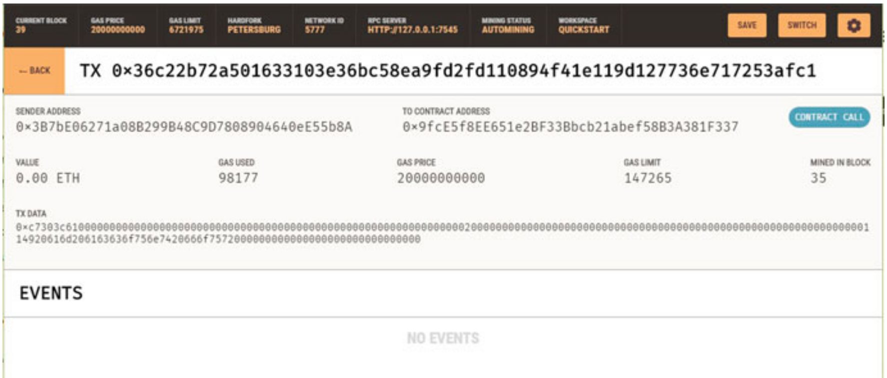
Local RPCs are utilized to interface between parts of the user interface written in JavaScript and the EHR manager written in GoLang. The EHR manager is fundamental for composing client information to the host file system. This incorporates usernames, passwords, and secret texts.

4.3 Ethereum Proof-of-Authority

Blockchain network was set up with three different systems. Each system represents the provider node, and each node was set into motion as a validator to the genesis block on the proof-of-authority (PoA) blockchain.

PoA is an algorithm the makes use of consensus mechanism that relied on the identity at stake. In PoA, an authorized account known as validator approved all the transactions and blocks chained into the network (Fig. 6).

In EHRMS, the validator provides a service known as the Ether Faucet, and the Ether Faucet is the fulfillment of the value of the ether required to perform



CURRENT BLOCK 39
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK PETERSBURG
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART

TX 0×36c22b72a501633103e36bc58ea9fd2fd110894f41e119d127736e717253afc1

SENDER ADDRESS
0×3B7bE06271a08B299B48C9D7808904640eE55b8A

TO CONTRACT ADDRESS
0×9fcE5f8EE651e2BF33Bbcb21abef58B3A381F337

VALUE
0.00 ETH

GAS USED
98177

GAS PRICE
20000000000

GAS LIMIT
147265

MINED IN BLOCK
35

TX DATA

```
0×c7303c610000000000000000000000000000000000000000000000000000000000000020000000000000000000000000000000000000000000000000000000000000001
14920616d206163636f756e7420666f7572000000000000000000000000000000
```

EVENTS

NO EVENTS

Fig. 6 Smart contract calls on the Ganache platform

a transaction on the network. Because of convenience, this process is obscure for system users. EHRMS requests for enough ether necessary to carry out transactions from a provider, for all transactions made by a user. This usually happens when patients perform their contract with an agent or when a provider becomes a validator. Providers that are validators automatically generate ether, as nodes endorse the blocks. Three specific types of smart contracts have been created, compiled, and deployed on the PoA blockchain to handle access control to EHR using a solidity programming language. The smart contracts are summary contracts, contracts for patient-provider relationships (PPRs), and contracts for registrars contracts. The compiler generates byte code, and each byte code is uploaded to blockchain EVM to represent a specific operation. The compiler generates byte code, and each byte code is uploaded to blockchain EVM to represent specific operation.

4.4 Storing EHR

A patient (P) has an encounter with a medical doctor (D) and the D generates a health record as EHRs for P. The D sends EHRs to P; upon acquiring the EHRs, P uploads the indexes of the EHR to the blockchain with the catalog of authorized user (U).

EHRMS allows each user to create a pair of keys during registration, the doctor (D) creates content extraction on EHRs using a pair of keys (pk, sk) and encrypt EHRs using symmetric key $\mathrm{k_d}$ for the purpose of confidentiality. All users in the blockchain network possess public key ($\mathrm{pk_i}$) and private key ($\mathrm{sk_i}$) to accomplish data sharing.

In our system, CES scheme is used to extract sensitive information from EHR to assure patient privacy. The doctor serrates EHRs into nine parts (name, age, sex, ID, contact, next of kin, medical history, diagnosis, prescription), and it is denoted as $M = \{m_1, m_2, m_3,\ m_4,\ m_5, m_6,\ m_7,\ m_8,\ m_9\}$. Then the doctor defines the content extraction access structure $CEAS = \{2, 3, 7, 9\}$ to avert virulent extraction. The process of content extraction signature is started by generating public/private key (pk, sk) using key generation algorithm. Next is for the D to sign the EHR data M using the signature extraction algorithm. After the completion of signature algorithm, the D encrypts EHR $(M, hi_{i \in [1,9]}, \sigma_F, CEAS, T)$ and patient's public key pk_p and sends both encrypted data to patient P.

$$\text{Message} = \left\{E_{k_d}\left(M, hi_{i\in[1,9]}, \sigma_F, CEAS, T\right), E_{pk_p}(k_d)\right\} \tag{1}$$

Upon receiving the encrypted data from D, P decrypt k_d and get M. The P uses CEAS to extract content of the signature and the corresponding EHR using signature extraction algorithm.

$$\text{Data} = \{(M_i, h_i, T), \sigma_E\} \tag{2}$$

P stores the extract signature and corresponding EHR in EHR manager and returns the storage location link. P partakes in the blockchain and anonymously by presenting the signed storage location link SIG_{skp}(Ind), and then a request (Rq) is sent to the blockchain where $i \in CI(M^{'})$ and t is timestamp.

$$Rq = \left\{SIG_{sk_p}\left(Ind_i\right), H\left(Ind_i\right), E_{pk_p}\left(Ind_i\right), t\right\} \tag{3}$$

$$Ind_i = (link_i, h_i, t) \tag{4}$$

After receiving, the request validator checks the validity of each transaction and collates all data during the period into a data set $Data_{set} = \{Rq, t\}$. The validator forms a new data block by hash the data set $Data_{hash} = H(Data_{set}, t)$, and digital signature $SIG_{sk_v}\Big(Data_{set}, Data_{hash}$. The validator broadcasts the data block to all the nodes on the blockchain.

$$Validator \rightarrow All : D_{block} = \left\{Data_{set,} Data_{hash,} pk_{v_i}, SIG_{sk_{vi}}\left(Data_{set}, Data_{hash}\right)\right\} \tag{5}$$

4.5 Sharing of EHR

To ensure save sharing of EHRs, P predefines access permission in the smart contract, i.e., access right and access activity, for instance, write, read, and duration of access. Smart contract is automatically prompted to run the corresponding operation once the predefined condition set is met. Data sharing process starts by initiating an EHR sharing request transaction (Rq) to the blockchain network. User U makes this request which includes the access target (ID), object to access (obj), and access content. Validators accept the transaction request and verify the U identity. If U is valid, the transaction will be stored in the blockchain.

$$U \rightarrow Validator : Rq = (ID, obj, ind, t), ind \in [1, 9] \tag{6}$$

If access conditions are met by the request, smart contract is prompted to decrypt the indexes of EHRs with patient private key skp and retires the cipher-text of indexes to U: else the request is rejected.

$$Message = E_{pk_u}\left(\text{ind}_i, t\right) \tag{7}$$

Table 2 Key recovery query execution time with varying database size

Key recovery/DB size	100 (ms)	1000 (ms)	10,000 (ms)
1	1.75	1.78	1.84
10	1.80	2.20	2.13
100	2.00	7.80	9.88
1000	4.38	11.00	13.12

5 Evaluation

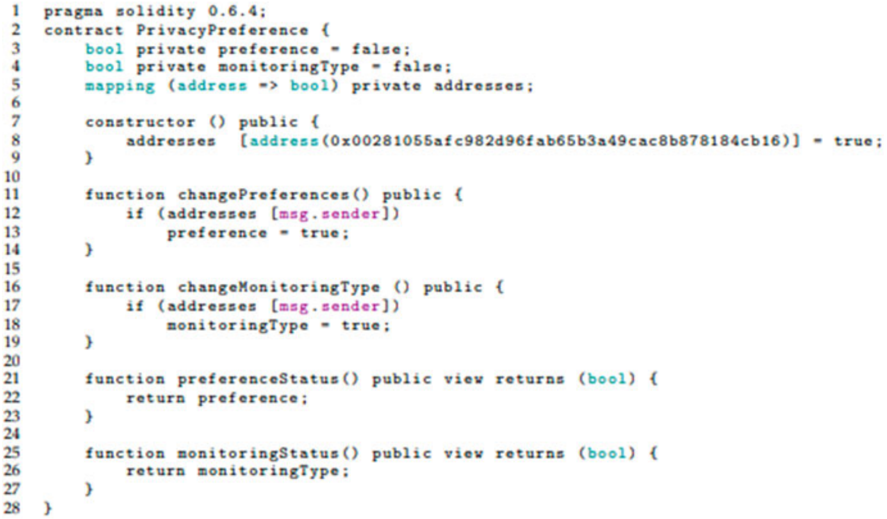
This section gives a performance study based on a series of experiments conducted to evaluate our system (EHRMS). We will first explain how the public key is obtained.

The first test was to determine a user's public key retrieval time connecting the EHR manager (gateway) database. We employed MySQL database system in the tests, on a host PC with Debian 9.8 OS, 4 GB RAM, and an Intel Core I5 1.6 GHz processor. Another machine running Ubuntu 18.04 LTS with 8 GB RAM and an Intel Core I5 2.3 GHz processor served as the EHR manager (gateway). Using three database sizes: 100, 1000, and 10,000 EHR, 1, 10,100 keys fetching time-taken was measured. For each database size, Table 2 illustrates the query execution time to obtain certain keys number. It is observed that the query execution time varies depending on the retrieved keys as well as the size of the database.

The contracts are developed and implemented in a private blockchain using Ganache and Truffle. Ganache, a personal Ethereum blockchain for developers' smart contracts, construct smart contracts, decentralized applications (dApps), test software, and inspect state while maintaining control of the chain. Truffle is an Ethereum virtual machine-based programming environment, testing framework and asset pipeline for blockchains (EVM). The first thing that was noticed during the network's construction was the maximum amount of gas that each block could hold. Ganache uses 6,721,975 gas blocks by default, while Main-net presently uses 8,000,000 gas blocks. We initially confirmed the gas cost of the smart contract we designed before setting the limit quantity of gas per block on the developed blockchain. The system executes an address mapping that changes a contract's privacy preferences, as indicated in the method in Fig. 7. The contract cannot be updated if the EHR manager determines that it does not include the requestor's address. We believe that one or more research institutions may request surveillance; thus each must have its own registered address.

A smart contract uses a certain quantity of gas, which is then stored on the Ethereum blockchain. We conducted studies to determine the gas cost of each contract by adjusting the number of addresses meet the user's privacy settings. Table 3 displays the results collected. As can be seen, the cost of gas rises as the number of addresses mapped in the contract grows. We picked ten addresses for each contract since storing values on the Ethereum network has gotten expensive.

The limit amount of gas is set for each block to store 10 contracts based on the value acquired in the previous experiment. Table 4 compares contracts saved in our



```
pragma solidity 0.6.4;
contract PrivacyPreference {
    bool private preference = false;
    bool private monitoringType = false;
    mapping (address => bool) private addresses;

    constructor () public {
        addresses  [address(0x00281055afc982d96fab65b3a49cac8b878184cb16)] = true;
    }

    function changePreferences() public {
        if (addresses [msg.sender])
            preference = true;
    }

    function changeMonitoringType () public {
        if (addresses [msg.sender])
            monitoringType = true;
    }

    function preferenceStatus() public view returns (bool) {
        return preference;
    }

    function monitoringStatus() public view returns (bool) {
        return monitoringType;
    }
}
```

Fig. 7 Privacy preference smart contract

Table 3 Gas cost varying the address quantity

Addresses	Gas cost
1	183,733 gas
10	320,090 gas
100	1,524,958 gas

Table 4 Contracts stored by block in different networks

Network	Gas cost
Default Ganache	11
Ethereum Main-net	13
EHRMS Network	10

network to those stored in Main-net and the regular Ganache network. The results demonstrate that the number of contracts saved in our network with Main-net and Ganache differs by a slight margin. Because the gas size of each block in Main-net varies over time, this variation has no effect on the network's functionality.

Then, a limit of 320,090 gas per block is established in our network, allowing us to store exactly 10 contracts every block. Because we employ a private blockchain, this value has no impact on network performance.

To register and verify the contract, the registration time of contracts in the blockchain was evaluated through the gateway, taking into account that each stored EHR refers to a contract. For this experiment, we used an Ubuntu 18.04 LTS system with 2 GB of RAM and an Intel Core i7 3.8 GHz processor to host our blockchain. By establishing a link with the blockchain, we next used the web3.js package to register and validate the contracts. Following that, we measured the time it took to register 1, 10, and 100 contracts. The results are shown in Table 5. We deduced from

Table 5 Execution time for contract catalogue in blockchain

Contract	Execution time (s)
1	0.63
10	4.80
100	39.20

Table 6 Execution time to obtain a contract in blockchain

Blocks	Execution time (s)
1	0.53
10	0.57
100	0.59

these findings that time-taken to register transactions in a blockchain varies linearly with the number of contracts being registered at the same time.

Following that, the address of each contract generated was used to search the blockchain for it and analyze the gateway's connection time to the blockchain. We ignored the time it takes for the gateway to retrieve the contract address from the database. As shown in Table 6, an increase in the number of blocks has no effect on the time it takes to obtain a contract recorded on the blockchain.

5.1 Security Assessment

We will assess the security of the developed smart contract in this part. We use a methodology to identify the primary sorts of attacks that can be carried out against smart contracts in this evaluation. We discovered three plausible contract assaults among them:

1. *Reentrancy:* Calling a smart contract function many times by different users can result in inconsistencies in the function's final result. We choose to use the change Preferences method for n different users in order to evaluate this attack in our contract.
2. *Front-running:* A changePreference() transaction can be observed in the platform's mempool (i.e., memory pool) before it is processed, allowing a person to react in advance. The memory pool serves as a repository for unconfirmed transactions. A transaction is created and then sent to the network and stored in the mempool. We want to check how numerous transactions in the mempool behave in our tests.
3. *Gas limit denial of service (DoS):* When a user attempts to exceed a block's gas limit with one or more transactions, the transaction is refused, and the transaction is not executed. In our experiments, we try to find an exploit in the contract that allows us to go above the gas limit.

To carry out the first sort of attack (Reentrancy), we used multiple addresses on the blockchain to call the changePreferences() function at the same time. We did this by registering the addresses that might have access to the blockchain in the

Table 7 Reentrancy attack result varying the number of addresses

Addresses	Expected result	Final result
2	True	True
5	False	False
10	True	True

Table 8 DoS probability in relation to contract complexity

Complexity	Probability of DoS
O(1)	Impossible
O(1)	High
O(n 2)	Extremely high
O(2 n)	Extremely high
O(n!)	Extremely high

smart contract. As previously stated, the maximum number of addresses that may be stored in a contract is ten; thus the test was limited to that number. We check whether the flow of calls to a single contract function can cause inconsistencies in it in this test.

According to the results obtained, the contract established was not influenced by the Reentrancy attack, as shown in Table 7. We discovered that the attack was ineffective due to the changePreferences() function's simplicity. This assault may have an impact on contracts with a higher level of complexity.

The Front-Running attack was carried done by observing the transaction mempool in Truffle Console and using the changeMonitoringType() method. We wanted to find the blockchain transaction in the mempool after running the method. However, because we use a private blockchain with few transactions, the function was executed immediately. As a result, there was no time to complete another transaction before the previous one was completed. Another factor contributing to this effect was the contract's simplicity, which shows that when the changeMonitoringType() function was called, a new block was formed. The Bloom filter record displayed tries to protect the user's privacy and defend against third-party attacks.

We investigated the contract to generate denial of service attacks in the third test (Gas Limit DoS). We used both contract's functionalities in this experiment. This test, unlike the first, seeks to generate an exploit in the contract in order to surpass the block's gas limit. Unlike the Reentrancy attack, which aims to maliciously change the value of a transaction using an exploit without exceeding the block's gas limit, this sort of attack prevents a transaction from being executed.

Based on the results of the tests, we discovered that the contract we built is tamper-proof against Gas Limit DoS. Because of the smart contract's simplicity, when a function is called several times, it is processed promptly, preventing DoS attacks. However, we discovered that the algorithm's complexity has a direct impact on this security concern. The created algorithm's complexity is classified as O(1), making the attack unachievable. When the contract design is not done appropriately, Table 8 shows the possibility of a DoS attack occurring based on the complexity of the algorithm.

To show the contract's intricacy, we utilized the Surya tool to create a graphic representation. Surya is a smart contract system utility tool that gives a multitude of visual outputs as well as information about the contracts' structure. It also allows you to query the function call graph for manual contract inspection. The contract functions do not interact with one another and cannot be invoked externally by other smart contracts. This method simplifies contracts and eliminates security concerns.

We used the audit tool Mythril to assess the security of the constructed smart contract, as we did in the previous experiment. Mythril is an Ethereum Virtual Machine bytecode security analysis tool. It employs symbolic execution, Satisfiability Modulo Theories (SMTs) solution, and taints analysis to uncover security issues in smart contracts. This program looks for code that could lead to inconsistencies in security and can uncover flaws in Ethereum and other platforms' smart contracts.

The security warning MythX SWC-103 appears in the report generated by the Mythril program. When we specify in the contract a distinct version of the pragma utilized in the compiler, a floating pragma is issued. Version 0.6.4 was used to create the contract while version 0.6.7 was used by the solidity compiler installed on the PC used in the tests. This technique can be problematic since old versions of the pragma can cause errors in the contract's execution. To fix the problem, we'll need to update the contract to utilize the same compiler version as the machine.

5.1.1 Privacy and Sharing

Patients' privacy is preserved by separating each patient's identity from provider identities. A new Ethereum account is created for separate patient-provider relationship by health providers. This enables the patient to establish public relationships with providers without exposing personal information of the individual who are involved in the relationships. But, communication is done indirectly via their provider's account; nonetheless, the account is for patients' transactions provision with ether.

Also, the system employs content extraction signature (CES) scheme to remove sensitive part of EHR signed by the doctors. CES generates the valid signature extraction which cannot be forged without the private key of the signer.

We restrict the amount of data to be stored on the blockchain to a small set by creating the reference the EHR. The references and predefine permissions are stored on the chain. It is important that every patient should have some data storage as on-chain. A 9727-byte executed transaction creates an identity catalogue contract. Thereafter, respective patient and provider relationship requires a 5007-byte transaction, with contract updates entailing 220 bytes. This effectively provides estimation of the required bytes for storage by every single node.

5.1.2 Storage Management

Blockchains need all the nodes to store information and links it to the blockchain because blockchain cannot save massive data. If these data are stored directly in the blockchain network, it will increase computational overhead and storage burden due to the fixed and limited block size. However, data privacy leakage is imminent. We restrict the amount of data to be stored on the blockchain to a small set by creating index of the EHR, which references the HER coupled with the index that is stored on the blockchain.

We apply the architecture for off-chain storage since it enhances large storage volumes of encrypted original EHR service provider local storage, and blockchain for on-chain verification only stores few indexes of the corresponding raw data. This reduces the blockchain storage load and private data integrity and privacy. Moreover, users can leave and rejoin the system at any time, and then get access to their historical record according to the index downloaded from the most recent block in the blockchain.

5.1.3 Data Audit

EHRMS also relies on audit log management as security mechanism since some exceptions may have resulted from the misuse of access privileges or dishonest behavior by data requestors. Audit log serves as proofs when disputes arise to hold users accountable for their interactions with patient record. Thus, immutable public ledger and smart contract in the blockchain provide immutable record for all of access requests to achieve traceability and accountability. Audit log majorly consists of important information such as timestamp of logged event, requester user, data owner ID, access type (create, query, update), and validation result of the request.

6 Conclusion

Electronic health record management systems rely on sharing architectures that are state of the art to maintain privacy. The design makes use of a private blockchain, smart contracts, and CES for anonymization. Because each patient's records are kept separate, their privacy is protected. For each patient-provider connection, healthcare professionals are generating a new Ethereum account to assist individuals in establishing public relations with providers without releasing personal information. Despite the fact that communication isn't done directly through the main account of their supplier, ether is also used to provide patient transactions. The system employs content extraction signature (CES) scheme to remove the sensitive part of EHR signed by the doctors. CES generates the valid signature extraction which cannot be forged without the private key of the signer.

As a web application, the developed system can be used on a variety of platforms, including PCs and mobile devices. By allowing all network nodes to check and disseminate all transactions and block them according to the established rules defined in the smart contracts, the system strikes a balance between security and comfort.

The use of decentralization concepts and blockchain frameworks to develop robust, user-specific, and interoperable EHR systems is demonstrated in this study. Data access is managed by Ethereum smart contracts, which keep verification logs and EHR entries and enable patients with comprehensive record reviews, care auditability, and knowledge exchange through multiple storage and provider networks.

The findings validated the viability of the architecture as designed. According to the outcome of the research, the applied smart contract is impervious to a variety of attacks. With regard to security considerations, the approach utilized in this work to build a basic complexity contract supported the proposed design. To be clear, more sophisticated structures may require even more complicated contracts.

In these situations, a more thorough security study is required in order to discover any weaknesses that could jeopardize the contract's correct functioning. The research presented in this publication builds on prior findings by Yue et al. [14]. It is worthy to note that emphasis is on the established architecture's security, converging entirely on the smart contracts structure, in addition to providing more details about the proposal and evaluating its performance. As a consequence of the performance and safety testing, we are able to show that the proposed architecture can be implemented.

References

1. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in *IEEE Open and Big Data (OBD) International Conference*, (2016), pp. 25–30
2. A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for Blockchain in healthcare: "medrec" prototype for electronic health records. Medical Research Data **13**, 13 (2016)
3. F. Arlindo, S.Flavio, R. Vladimir, L.Angela, and M.Marcos, Electronic Health Records using Blockchain Technology. Future Internet for Smart Cities funded by CNPq, 2018, proc. 465446/2014-0, CAPES proc. 88887.136422/2017-00, and FAPESP, proc. 2014/50937-1
4. D. Alevtina, X. Zhigang, R. SamueL, S. Michael, W. Fusheng, Secure and trustable electronic medical records sharing using blockchain. AMIA Ann Symp Proc, 23 (2017)
5. L. Jingwei, L. Xiaolu, Y. Lin, Z. Hongli, D. Xiaojiang, G. Mohsen, BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. IEEE Glob. Commun. Conf. (GLOBECOM), 22–27 (2018)
6. S. Alexaki, G. Alexandris, V. Katos, N. Petroulakis, Blockchain-based electronic patient records for regulated circular healthcare jurisdictions, in *IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks*, (2018) https://ieeexplore.ieee.org/abstract/document/851495
7. A. Siyal, A. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography (2019). https://doi.org/10.3390/cryptography3010003

8. L. Wanitcharakkhakul, S. Rotchanakitumnuai, Blockchain technology acceptance in electronic medical record system, in *Proceedings of the 17th International Conference on Electronic Business*, (2018), pp. 53–58
9. Q. Xia, E. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Published in Information. (2017). https://doi.org/10.3390/info8020044
10. M. Holbl, M. Kompara, A. Kamišalic, A. Zlatolas, A systematic review of the use of blockchain in healthcare. In symmetry. (2018). https://doi.org/10.3390/sym10100470
11. A. Rajput, Q. Li, A. Ahvanooey, I. Masood, EACMS: Emergency access control management system for personal health record based on blockchain. IEEE Access **7**, 84304–84317 (2019)
12. D. Nguyen, P. Pathirana, M. Ding, A. Eneviratne, Blockchain for secure EHRs sharing of mobile cloud based E-Health systems. IEEE Access **7**, 66792–66806 (2019)
13. R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access **6**, 11676–11686 (2017)
14. Y. Xiao, W. Huiju, J. Dawei, L. Mingqiang, J. Wei, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**, 218 (2016). https://doi.org/10.1007/s10916-016-0574-6
15. K. J. Peterson, R. Deeduvanu, P. Kanjamala, & K. Mayo, “A blockchain-based approach to health information exchange networks”, 2016.
16. Y. Huihui, and Y. Bian, “A blockchain-based approach to the secure sharing of healthcare data” 2017.
17. A.J. Zargar, M. Manzoor, T. Mukhtar, Encryption/decryption using elliptical curve cryptography. Int. J. Adv. Res. Comp. Sci. **8**(7) (2017)

An Investigation of Blockchain Technology and Smart Contracts Deployment in Smart Medicine 4.0

Anna Polubaryeva

1 Introduction

1.1 Smart Life

Currently, almost all areas of human activity are becoming "smart": this means that everything is interconnected and digitalized, and a large number of software, devices, equipment, technics, technicians, and other various staff are used in order to carry out activities in a separately taken area. Medicine is not an exception at all; on the contrary, it is one of the advanced areas that are on fast forward toward an Industry 4.0. Smart medicine occupies a special place in the smart ecosystem, also because it belongs to the critical infrastructure in any state. This means that it not only receives the close attention of governments and society but also is in a great demand from population who is the main user of this critical infrastructure. In the field of "medicine," the Smart Medicine 4.0 has its unique space as well: it is the latest and the most important part of medicine, which is developing, although not rapidly, like other industries, but progressively and confidently. Transition to "smart" medicine is now a priority in many countries.

At the moment, the transition from Industry 3.0 to Industry 4.0 has just begun, and although the healthcare sector is making this transition gradually, the pace of this transition is not as quick as, for example, in other sectors, such as manufacturing

Part of this work was done when the researcher visited the University of Nicosia under the Erasmus Student Exchange Program.

A. Polubaryeva (✉)
Secure Information Technologies Department, ITMO University, St. Petersburg, Russia

Department of Computer Science, University of Nicosia, Nicosia, Cyprus

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_10

and logistics. A satisfactory transition is observed primarily in the countries that are pioneers and leaders in the transition to Industry 4.0 paradigm and, in particular, to Smart Medicine 4.0 (Germany, Italy, other EU countries, the USA, the UK, and China). Thus, it could be concluded that smart medicine has many challenges to be addressed as well as positive and negative aspects.

1.2 Smart Contracts

Smart medicine is developing and/or is under development in many countries. The use of blockchain and smart contracts in medicine was proposed from the very beginning; however, it is only over the period from early 2010 to the present that the idea of using blockchain and smart contracts in the field of smart medicine has grown incredibly. Many countries now develop the overwhelming blockchain ecosystem for healthcare, the one of the largest is in the EU [1], which intends to embrace the broad number of initiatives and deployments offered by the blockchain researchers. Various use cases, schemes, and ideas for these technologies have been proposed, including hybrid ones, for example, using federated learning and machine learning [2]. And one of the most intriguing and practically applicable challenges is to provide, as well as increase, the level of security and privacy.

Speaking of security and privacy of the healthcare sector, it shall be noted that the methods proposed for the protection of security and privacy are currently very diverse and sometimes based on opposite concepts and principles. For example, there are opponents for using decentralized systems as a foundation for the smart medicine framework, whereas others insist on centralized systems. Privacy enhancement techniques [3–6], federal technologies [7], fog technologies [8], big data methods [9], and different hybrid methods are offered apart from blockchain-based methodologies.

And if initially the priority was simply to use a verification function of the smart contracts in smart medicine, nowadays, the use of blockchain for the purposes of improving the quality of life for disabled people and tracking Covid-19 does not seem to be something surprising [10]. In addition to the tasks of direct participation in the provision of medical services (in one or another manner and scope), smart contracts and blockchain are very actively proposed for implementation to ensure security and privacy in the smart medicine paradigm (for devices, hospitals, medical data storage systems, etc.). However, it is a blockchain that is the better solution among all other possible options due to its inherited and built-in functions and abilities. Thus, the results of studies by various authors (academicians and practitioners) show that due to their unique qualities, blockchain and smart contracts can significantly improve the enhancement and support of privacy and security in the healthcare sector. In this chapter, smart contracts and blockchain technologies for smart medicine will be discussed.

The rest of the chapter is organized as follows: Section 2 gives a brief description of the blockchain technology and its specific elements (e.g., smart contracts) while at the same time discusses its main characteristics, advantages, and disadvantages. Section 3 presents the findings of a thorough and detailed investigation of the blockchain and smart contract applicability in the healthcare sector. Section 4 concludes. The term “actors” used throughout this chapter includes all the participants involved or may be potentially involved into the smart medicine ecosystem.

2 Current Blockchain Technology and Smart Contracts Issues and Challenges

2.1 Blockchain and Smart Contracts in a Nutshell

Before moving on and revealing the benefits of blockchain for security and privacy, including for the healthcare sector, it is necessary to give a brief description of this technology and its specific elements, such as a smart contract, as well as illustrate its main characteristics, advantages, and disadvantages.

Blockchain is the tool that currently best ensures the security of the Internet of Things (IoT) and medical devices included in it. The blockchain has specific characteristics such as peer-peer communication, transparency, trust, immutability [11], auditability [12], and autonomous workability (it can work without any additional trigger). The combination of these characteristics makes it one-of-the-kind tool which allow using it in many areas: cryptocurrency and blockchain technologies provide a unique opportunity for various spheres and industries to use this technology not only for the deployment of businesses, services, and applications but also for the provision of high protection equipped with cryptographic methods and algorithms. And this makes blockchain and Ethereum in particular an excellent tool for softening security issues during the deployment of smart contracts. The Ethereum is considered by many as the best blockchain platform which may be used for various purposes.

A blockchain is a system that serves as a tamper-proof ledger distributed on an assemblage of communicating nodes, each and all of which shares the same genesis block – an initial block of information, which has no parent block. In order to add information to the blockchain, a node includes information in a block with a pointer to its parent block; this creates a chain of blocks and hence called blockchain. One of the important components of blockchain technology is the mining process, which is as follows: a node solves a crypto-puzzle and provides the solution as a proof of its work to get a reward [13], and as a result, the new block is created. This new block will be used in the future transactions and creations. There are few platforms for developing blockchain-based application: Ethereum, R3 Corda, Hyperledger Fabric (HF), Quorum, Hyperledger Sawtooth, Ripple, and so on.

Since 2008, there are a lot of research, experiments, and proposals on the topic of blockchain, smart contracts, and cryptocurrencies. Initially the blockchain was supposed to be used only for payments between peers; however, over time, the technology was proposed to be used for all sorts of other purposes, such as distributed storage and academic research on consensus protocols, and one of such applications is to enable the smart contracts [14].

The smart contract can be defined as a self-executing financial instrument that synchronizes its state through blockchain transactions, may interact with decentralized cryptocurrencies, has its correct execution enforced by the consensus protocol, and takes user contribution. In the Ethereum environment, it may also be considered as an autonomous agent executed by an Ethereum virtual machine (EVM) and is the core foundation and the main building blocks of any distributed application (DApp) [15]. Giving a basic description, smart contracts are small, terminating, deterministic computer programs written in a high-level language like Solidity or Viper, or it can be described as a piece of code that executes on a blockchain. The computation and state are all public. The Solidity is an assembly-like, contract-oriented, stack-based, quasi-Turing complete language which consists of 65 unique opcodes [16] and is the most applied one for developing of smart contracts. In Ethereum network, when a code is deployed on the blockchain, the EVM is going to run it as long as the conditions apply; moreover, the triggering functions in the smart contract may be executed from any account only if two conditions are met: address of the smart contract is known, and the function caller has enough Ether to trigger. Smart contract has the ability to aggregate user votes, negotiate with other contracts, store and represent tokens and digital assets, and make and receive cryptocurrency payments. Smart contracts have an important benefit because they provide a significant added value: the code handling the business logic in it is not so vague as in conventional servers, and getting public, thus, is going to be easily verifiable.

2.2 Advantages in Comparison with Non-blockchain Systems

2.2.1 Generic Blockchain Advantages

Despite all challenges blockchain and smart contracts demonstrate at the moment, blockchain technology has undeniable advantages over non-blockchain systems. These benefits can also be used for security, privacy, and other aspects in various ways. *These advantages are, in particular, as follows*:

(a) The secure storage of the ledger data and the transactions using the special structure based on both encryption/hashing and Merkle tree. This structure also ensures integrity of the data stored in the blockchain [17]. All cryptographic algorithms in blockchain increase the data security as each block contains the cryptographic hash of the previous block.

(b) Low cost of the maintenance [18] – the execution is getting automatic after the smart contract was deployed.

(c) Immutability and traceability of each transaction in the network, where each operation is recorded, logged, and hashed; thus, it is easy to carry out an audit of the transactions, including unwanted or unlawful ones [19].
(d) The databases are less vulnerable to attacks due to the unchangeable nature of the blocks in the blockchain; thus, it can provide strong immutability.
(e) A distributed peer-to-peer architecture which allows the blockchain system to control and eliminate a single point of failure. Hence, the low (or reduced) risk of the failure due to the decentralized and distributed nature of the blockchain.
(f) Not only the accounts encrypted with high security but also externally owned account (EOA), being an anonymous account, protects the identity of the owner because it is not possible to determine such an owner of the account and their data attached; consequently, the blockchain provides higher confidentiality and privacy for the account's owner.
(g) A unique business logic of the smart contract, which allows its use in any possible field [19].
(h) All nodes in the blockchain have a copy of the blockchain with all transactions recorded in it in keeping, and this means a higher availability of the data stored in the blockchain.
(i) The higher level of the flexibility of the environment for the run time of devices and IoT devices due to the lack or rareness of the single point of failure mentioned above [20].
(j) Infeasibility. The blockchain system is extremely robust due to the distribution of the copies of the data through different locations [18].
(k) The design of the blockchain aimed in general to provide integrity and availability: each block stores all the transaction data. The integrity of data in the blockchain ensured by the Merkle tree form of the nodes [17].

2.2.2 Blockchain Advantages for Healthcare Industry

The following ways of using blockchain to provide a higher level of transparency and trust among actors of the decentralized IoHT system and Medicine 4.0 can be highlighted at the moment:

(a) With the execution of the smart contract and EOA, patients and other covered entities may control and check the data related to their health and verify many actions and operations, for example, if they are still patients of the hospital.
(b) Smart contracts in the blockchain enables an abstraction layer which helps to the various healthcare providers and other healthcare-related entities that have different electronic health records (EHRs) and privacy/security standards to be in a secure and constant communication and transfer the data using this layer [21].
(c) Healthcare industry may be benefited by such a characteristic of the blockchain as interoperability: the EHR and other data stored in the blockchain in the IoT

have a content-wise interoperability caused by the ability of the IoT to transfer the same data from one node to another [22].

(d) A decentralized nature of the blockchain allows all actors of the healthcare industry to participate limitlessly in healthcare data transmission as well as provides excellent availability and resilience of the data and operations.

(e) The blockchain-IoT ecosystem with different tools of secure transmission of the data is going to help to reduce the general cost of the data transfer in the healthcare.

(f) Data sources of EHRs can be secured with greater power since CIA triad (confidentiality, integrity, and availability) will be enhanced by the decentralized storage method provided by the blockchain network and its nodes. Each CIA component in healthcare system may be benefited by the blockchain as follows: encryption techniques help to increase a data confidentiality, hash values will provide healthcare records and information with data integrity, and data availability becomes easier in the blockchain environment than in traditional health ecosystems [23].

(g) The usage of the blockchain technology will guarantee faster healthcare services and products providing and supplying since the blockchain may provide IoT healthcare facilities and patients with the advantages determined by the decentralized nature of the blockchain, namely, the ability of the nodes to transfer information quicker. Additional tools, for instance, wearable IoHT devices and such configuring cellular technology as LPWAN or 5G, may increase the speed of transmission [23].

(h) The immutability and transparency features of the blockchain can assist in retaining the medical and personal data of the patient in an intact block and assimilate the genuineness of ongoing e-healthcare services, respectively. Furthermore, actors may participate in the entire process to designate the validation of transparency [22].

(i) Constant real-time update of the information stored in the blockchain network that gives an advantage to the blockchain in healthcare industry, where fast transmission of data is crucial [21].

(j) The blockchain may suffuse IoHT by adding improvements to system integration, coherence, confidentiality, and compliance [24], because usually the blockchain consists of two elements: *transactions*, which are the operations made by the participants of the BC, *and blocks*, which record the transactions and guarantee its arrangement is unmodified.

(k) The tremendous and crucial advantages of the blockchain and smart contracts for healthcare industry, one can generally consider, are the wide scope of blockchain applications in the multiple actions which can be performed in Healthcare Industry 4.0 using blockchain network [25–27], such as research incentivizing, the blockchain-based access control, consent management, key management, claims management, data verification, narrowband IoT device management, etc. Some of these applications will be considered later in Part D of Sect. 2 of this chapter.

(l) The medical data shared among the different healthcare actors, combined with new smart labels that use the IoT to remind and track a patient's treatments, would give extremely helpful data not only for health professionals but also for machine learning algorithms of the AI analyzers aiming to give more personalized treatment and, hence, will lead to improvement of the healthcare and security mechanisms [28].

2.2.3 Blockchain and Smart Contracts Challenges

Blockchain, as a means of protection against attacks on IoMT and IoHT, is proposed by modern researchers quite actively, especially in the last 2 years [3, 19–22, 24, 29–45]. In addition, blockchain and smart contracts are recommended to be applied in various areas, as mentioned above. Despite the prospects and many positive aspects, blockchain also has its own shortcomings, which must be identified in order to try to overcome them in the future. Blockchain in the IoT and IoHT environments is facing the following challenges [29, 46]:

(a) *Storage facility stringency challenge*. The needed storage capacity in the IoT context is far lower than the ledger-based blockchain technology for sensors and actuators. IoT allows for the processing of a single central database, where each ledger must be saved at each node, similar to blockchain. When compared to regular IoT devices, it consumes greater space over time.

(b) *Lack of facilities challenge*. This issue seems a minor one; however, if not to address it in a proper manner, it may cause the limitations in blockchain and smart contracts implementation into the majority of the IoT projects.

(c) *Privacy and reputation challenges*. These issues are considered as the major negative sides of the blockchain due to the fact that it is not only data persistently stored on a ledger, but the whole network has an access to such a data because of the nature of the blockchain, which is pseudonym and can protect the users' identity; however, the privacy and reputation can suffer because of analytic methods which exist in the blockchain (crypto-puzzle, consensus algorithm, etc.). These methods can lead to traceability of the transactions to a specific identity of the owner of the account or other assets in the blockchain [3].

(d) *Manpower challenge*. There are not many efficient and qualified employees who are familiar with the blockchain and smart contracts technology.

(e) *Processing time challenge*. The authentication process can take various time slices due to the difference in the computational capacities of the peers in the blockchain which can lead to the different processing time. Thus, unpredictability becomes a new challenge that may lead to impossibility to build new schemes, processes, and infrastructures with blockchain implementation.

(f) *Scalability challenge*. Concerns about the permissionless blockchain platforms' scalability are a major hiccup to their widespread implementation. The limitation on the scalability means that Ethereum platform has a limited maximum transaction throughput [47, 48], which is caused by the such inherent feature of the blockchain as linear raise of the time to process individual transactions while the number of the participants grows. The main trigger for the choice of the transactions to be included into the blockchain is the decision of the miners, whose main desire (mostly) is to gain more money. Thus, this restrain the scalability as well as a bootstrap time [48], and lack of consensus finality – the time needed for a new node to download and process an entire transaction history. The lack of consensus finality is another key factor of influence on scalability (toward "scaling out of scaling") and the ability of new nodes to join the network [49]. However, there are many research works and proposals that exist by now and continue to grow, related to the methods which allow to override this scalability problem [49, 50], for example, with the use of such techniques as plasma and sharding that make it possible to create a parallel performance of the transactions and, consequently, increase tremendously the workability of the blockchain platforms with the implementation of the data partitioning [50].

(g) *Legal issues*. There are no legal acts in the USA, the EU, and other countries which regulate the blockchain and smart contracts in a full manner and allow to control them. The authors in [29] consider this problem as the most significant drawback. The lack of the proper legal regulations may trigger many problems if infrastructures or institutions implement blockchain technology without consistent legal framework and support, due to the fact that any new technologies may lead astray the initial intentions.

(h) *Mandatory observance of certain conditions for the operation of the blockchain*. In [19], a number of limitations of blockchain usage are mentioned. The peer nodes execute set of functions, which allows operating on the ledger data and performing powerful complex operations. Blockchain cannot be used in every system; there are a few requirements that must be completed before a blockchain-based architecture can be deployed. There are crucial conditions and terms that must be considered while using the blockchain: need for sharing of data; need for immutable logs of operations occurred; multiple actors involved in the system; whether there is a leader or a group of leaders controlling the system on which the system is trusted, and whether there are uniform rules throughout the participants. Moreover, there has to be significantly less chance of amendment of the rules and norms of the transactions.

(i) *The serious bugs in smart contracts itself*. It includes anything from transaction-ordering requirements to exceptions that have been mishandled. The EVM provides inter-contract execution to allow reuse of code via calls to library contracts, thus complicating the existing difficulty of getting high certainty [51].

(j) *Privacy leakage and selfish mining related to consensus algorithms proof of work (PoW) and proof of stake (PoS)* [37].

(k) *Absence of the thoughtful standardization and sufficient official policies in healthcare industry*. There are few standards by now developed by blockchain communities and associations (for instance, ISO 22739:2020 Blockchain and DLT, ISO/TR 23244:2020, ISO/TR 23576:2020) and few are under development; however, the blockchain and other professional's communities are still in the process of creating proper and sufficient standards for blockchain and smart contracts usage and implementation into mundane working procedures of different infrastructures and application to the various areas.

2.2.4 Security of IoT and IoHT Critical Infrastructure: Blockchain as a Solution

The issue of digitalization of all sectors of the economy and the transition to “smart” industries and “smart” social infrastructures is increasingly being discussed, but in reality, movement in this direction is proceeding very slowly; however, this does not mean that it is not worth working out security issues now: the sooner the problems are identified and possible and potential solutions are found, the easier it will be in the future to build a competent information security protection system in the healthcare sector.

The situation with regard to information security in healthcare remains constant. The predictions made by the researchers until 2020 were fully confirmed: the authors [52] indicated that the healthcare sector generates a tremendous scope of data which is under operation every second. For example, the worldwide medical data exchange and traffic for a year 2020 was approximately 2314 exabytes. This prediction came into life, and nowadays, it is predicted to be growing every single year. Such a large amount of valuable data attracts cybercriminals, who are increasingly monetizing healthcare data.

According to the forecasts of the authors of [53], the growth of cybersecurity market in healthcare industry is expected to reach USD 27.10 billion by 2026. Why medical data is valuable? The medical data, as noted by both academics and companies specializing in cybersecurity, becomes an object of great value due to its pure nature, since the information security of medical institutions, medical devices, and personal data of the patients is the security matter of every single person in the world. Studies show that the price of medical data, including information about patient health data, is 50 times higher than financial information. The cost of one medical card can be as high as $60 on the black market, which is 10–20 times more than credit card information [54]. According to forecasts [54], in 2019, healthcare should have been subject to 2–3 times more cyberattacks than the average for other industries, and these forecasts came 30 true. Inadequate security methods, weak and generic passwords, and vulnerabilities in the code open the way for attackers to manipulate the data of healthcare institutions. In addition, with the development of the use of cloud technologies and IoT systems in healthcare, their vulnerability is growing. According to [55], in 2019, “smart healthcare” is the leading target for cybercriminals. As noted earlier, in most countries, healthcare is classified as a critical infrastructure, which means that the interest of attackers doubles: not only material values are at risk but also the well-being of citizens of a particular country. “Criticality” or importance also grows due to the fact that biomedical research generates valuable data, there is an active exchange of medical information between medical institutions over computer networks, the medical environment (healthcare environment) becomes associated with many systems, and, accordingly, cybersecurity problems are also growing and require immediate resolution and response. The general trends in data storage have also changed, and it is now difficult to ensure the resilience of security systems with the current growth of cloud infrastructure and the IoT. If the gradual introduction of connected medical devices, digitalization, and the development of smart hospitals takes place around the globe, it is necessary to foresee all possible risks in advance, using the most prospective and effective technologies at hand, such as blockchain and smart contracts. Due to its positive and even negative moments (what can be eliminated and developed into a benefit), blockchain is the cast of the role of the instruments for solving problems in many aspects and economic sectors.

2.2.5 Summary

It could be argued that the use of blockchain and smart contracts in Smart Medicine 4.0 is, if not mandatory, then definitely an advantageous technology that can be implemented at all levels of the healthcare system, to all types of actors, and to improve any devices and equipment. Section 3 will consider in more detail the ways of practical application of the blockchain and smart contracts. As will be shown further, the ways of developing the smart medicine with the introduction of blockchain technologies and smart contracts in full or in part are different and can be applied by each individual healthcare facility depending on its needs, tasks, and problems it faces.

The main advantage of "smart" medicine is that it includes elements and advantages (though also disadvantages) of digitalization and cyber-physical systems. The main advantage of using blockchain and smart contracts is that if the shortcomings of these technologies are overcome or mitigated (in the future), then the degree of security in the healthcare sector, as well as the level of their overall development by accelerating many processes (authentication, data transfer, etc.) with the help of blockchain, will grow exponentially. In fact, smart medicine with smart contracts is doubly smart medicine. And this is an advantage for every single person on Earth.

2.3 Legislation and Legislative Initiatives Related to Blockchain and Smart Contracts in Different Jurisdictions

Legislation on the blockchain, smart contracts, healthcare, and smart medicine is also important, as it reflects the already existing trends and sets trends for the future and also reflects all the challenges that are facing the smart medicine industry.

2.3.1 General Legal Regulation Provisions of Blockchain and Smart Contracts

Currently, the legal status of blockchain and smart contract, as well as the definition of their legal nature, remains an open question. After an in-depth study of the legislation of various countries, it can be argued that the blockchain and the smart contracts, unlike cryptocurrency, tokens, and ICOs, are not properly regulated by law; moreover, even relatively good recommendatory acts are absent. Some believe that the reason for this is the reluctance of the state authorities of some countries to let economic leverage out of their hands and allow the development of decentralized economic relations [56]. This is indeed the case, as states prefer to use already accustomed, traditional instruments, since new tools always bring more risks and unpredictability and may affect an economy and people.

The only country in which the court has recently issued a precedent decision, according to which the smart contracts were equated to ordinary contracts, is the Great Britain [57]. However, this still does not cover the entire field of activity and application of the smart contracts; accordingly, there are still many questions and problems to be resolved. In other countries such as the USA [56, 58–62], EU [63–65], and Canada [66–69], mainly in the legislation, it is said about cryptocurrencies, ICOs, and ITOs, and only general definitions of smart contracts and blockchain are given without any details [70]. Work on the study, development, and application of the blockchain and smart contracts in various countries is being actively pursued; many state bodies and committees have been created. However, up to now, completed and full-fledged laws and regulations have not been adopted or approved. The study also showed that legislation on the use of smart contracts and blockchain in healthcare is also not currently adopted, despite the fact that in the state of Virginia [71], an act has been adopted that is aimed at creating the healthcare provider credentials data solution ruled by the Department of Health Professions and shall solicit proofs of concept to establish or improve a system for the storage and accessing of healthcare provider credentials data, utilizing blockchain or a similar technology. However, despite the fact that this is the only act in the world at the moment that at the state level mentions the possibility of using blockchain in healthcare, it is still a declarative act consisting of one article.

The legislative consolidation of the status of smart contracts and blockchains in healthcare was also not found according to the results of a large study of different laws, regulatory acts, and so on, although, for example, the use in agriculture has already begun to be legislatively developed in the state of Colorado [72]; in the states of Connecticut and North Dakota, a campaign on the use of blockchains and smart contracts for votes and elections [62, 73] started; in Nebraska, the same is in the insurance industry [62]; etc.

2.3.2 Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The most elaborate rules are the HIPAA Regulations for a healthcare sector, which contain the broadest list of actors and companies providing healthcare services. The main concept that exists in HIPAA is the concept of "subjects" – covered entities. The introduction of this concept is fundamental as it helps to understand which organizations must comply with the HIPAA requirements. Covered subjects are healthcare providers (namely, doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, but only if they transmit any information in an electronic form in connection with a transaction for which the US Department of Health and Human Services (HHS) has adopted a standard), a health plan (namely, health insurance companies, HMOs, company health plans, government programs that pay for healthcare, such as Medicare, Medicaid, and the military and veterans' healthcare programs), and a healthcare clearinghouse (includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa) [74]. Covered entities are subject to HIPAA checks conducted by the Office for Civil Rights (OCR) of the Ministry of Health and US Social Services (OHS), that is, these are the very individuals and organizations that must strictly adhere to the HIPAA Rules. Facilities and companies that have agreements with HIPAA are business partners that legally obliged to handle protected health information (PHI) in a manner that is consistent with HIPAA's Privacy and Security Guidelines.

The second important HIPAA group is a group of actors called the business associates, which includes third-party providers who provide services on behalf of one of the covered entities actors that require access to or use of protected health information (PHI). It should be noted that directly in the HIPAA regulations, companies such as AWS, GCP, and Azure are classified as business partners, that is, some software companies are immediately named in HIPAA and designated as actors. Even the insured risks of the healthcare provider and the business partner depend on the extent to which they comply with the HIPAA Rules: covered entities must demonstrate their cybersecurity to minimize the likelihood of inadvertent disclosure of PHI in the event of data and information breaches [75]. Vendor risk management is a particularly important part of cybersecurity risk management for organizations that employ third-party vendors. Before entering into any agreements with business partners, healthcare organizations must complete a cybersecurity risk assessment to understand how the business partner is managing information security and whether it is HIPAA compliant.

2.3.3 General Data Protection Regulation (GDPR)

Unlike HIPAA, the GDPR [63] focuses on personal information. There, the classification is made according to the following principle: depending on the legal status, these can be public and private actors (cl. 5 of the GDPR) – that is, these two categories include both natural persons (e.g., patients) and all possible organizations (e.g., healthcare providers and various service providers).

Depending on the functionality performed, this is a data subject, a data controller (or joint controller), and a data processor (chapter 4 of GDPR, cl. 45). The data subject is a person/entity which obtains an identifier that can include name and location. In healthcare, these are mainly patients and their representatives. The data controller is a person/entity that manipulates with personal data: specifies operations or processing activities (cl. 7 of GDPR). In healthcare, this can be all healthcare providers and any person providing healthcare to a patient. The data processor is the analyzer of the data subject's data on behalf of a data controller or joint controller. This, for example, could be AI analyzer, IoMT device, and so on. Health issues are separately mentioned in the GDPR (cl. 45), where they are named among other components of public interest. However, in addition to referring healthcare to this category of cases and specifying under which law the controller should act, the GDPR does not contain specific provisions or specifics of regulation in the healthcare industry or cases.

2.3.4 Smart Medicine as a Target: The European Union Agency for Cybersecurity (ENISA) Recommendations

The recommendation document for providing a professional degree of information security in smart hospitals was developed by the European Union Agency for Cybersecurity (ENISA) [76]. These recommendations have a huge practical orientation and deep study of information security issues in smart hospital. The smart hospital of the future will function exactly as a single organism that absorbs all types of actors, devices, and services, which accumulates not only all types of assets but also all types of information (medical, personal, and financial data). The smart hospital is a basic unit for the future smart medicine paradigm.

Interconnected clinical information systems and networked medical devices are named as two cornerstones of the smart hospitals due to its position on the smart hospitals: they are new IoT elements that support and provide the work of the entire hospital. According to clause 2.2 [76], many hospitals are now becoming smart hospitals that are intelligently connected and have autonomous decision-making mechanisms. Smart hospitals have a tremendous scope of assets (mainly tools and equipment) which shall be considered not only as a part of cyber-physical system but also as a part of the smart medicine.

It is also worth noting that in these recommendations, the concept of data is considered and presented in more detail. Among other things, the documents regulating the activities of ENISA provide for the need for certification in the field of cybersecurity, which creates the need to introduce any actors of certification bodies into the interaction scheme.

ENISA has also developed currently new recommendation documents related to:

1. The Cloud Security for Healthcare Services (where cloud service provider and customers aka healthcare organizations, cloud service provider, and medical device manufacturer are presented as a separate group of actors). Moreover, there are separate types of healthcare cloud services – nonexhaustive overview of the currently identified cloud solutions for healthcare systems: enterprise resource planning systems (ERP systems), health information systems (HIS), communication services, office management, cloud-based network, health data analytics, medical devices, telemedicine services, medication monitoring, and supply chain management [77].
2. The Procurement Guidelines for Cybersecurity in Hospitals [78].
3. The Security and Resilience in e-Health Infrastructures and Services [79] (their recommendations are directed to: public institutions responsible for e-health strategy, e-health competence centers, e-health platform operators, academia, user associations – networking organizations, standardization bodies, ICT industry (suppliers). In this infrastructure the patient and the healthcare professional are highlighted.

3 Internet of Health Things Blockchain and Smart Contracts

During the past few years, IoMT showed a tremendous increase that led to the massive researches in the field of application of the blockchain in the healthcare ecosystem. This is also conditional upon the fact that all medical and personal data of the patients are highly valuable as they can be of great importance to all stakeholders within the healthcare industry. The recent and leading-edge relevant works of different technical teams all around the world have various focuses; however, the main conclusion that can be made is that nowadays the majority of the authors agreed and proved that the blockchain is a future instrument to increase the level of security and privacy in the IoHT. About 60 works were studied on the application of blockchain or mixed blockchain techniques, and in this chapter, the most interesting ones are presented shortly for better understanding of the blockchain role in the development of IoHT and protection and enlargement of its security.

3.1 Attacks on the Healthcare Sector: Defense on the Base of the Blockchain

The general scheme using the blockchain technology and one-time password (OTP) in healthcare against attacks was proposed by the authors of the work [29]. The main essence of this scheme is that tokens are used for security and privacy – they have a short life period and are constantly updated, giving access to patient’s data to the patient himself or to third parties (authorized ones). The proposed scheme describes the login process of the user using tokens and the mechanism of its usage. The token shall be generated each time when a user tries to sign in into “patient’s database” – but nothing is said about how this database is created, how actors get access to it, what this database ultimately contains, and what kind of information about the patient is stored in this database. The authors’ proposal in fact is that for intrusion detection, it is enough that token’s short activation (for a determined amount of time) on the blockchain public or private network will suffice to resist a cyberattack. For prolongation of the access, a new token has to be generated. In addition, they offered that the token serves as a dummy number that contains a personal information of the user which is encrypted with the help of the hash function and stored in blocks. The authors neither specify how it works nor what mechanisms are used. In addition, it is not specified whether the patient’s medical information is included in the personal information, what exactly it consists of, and what role Wide Area Sensor Network (WASN) plays in the scheme.

OTP proposed in this work is rather advantageous issue; however, it can be also considered as a disadvantage, because it can make it difficult to work with medical data (constantly entering a password is very difficult and sometimes fraught with loss of time). Moreover, the description on the detection of attacks (external and internal in healthcare institutions) using blockchain is well performed. The main drawback of this work is that it is focused on the network layer and has no detailed distinction of the persons who can enter the IoHT. The authors indicated that with the blockchain encryption mechanism, it will ensure the security of the information stored in the token and the user’s information as well as information on detailed user’s operations within one session (connection to the database of the administration).

3.2 IoT-Blockchain-Based Monitoring Model and Smart Contract as a Verification Link for Smart Healthcare Purposes

A more cryptographical angle is presented in [30] *where it was proposed to use the following model*. Wearable medical devices (WMD) are equipped with cryptographic protection, namely, the implementation of the smart contracts installed on PC or patient’s smartphone, which can make an analysis of the gained and formatted medical data of the patient. Moreover, an *IoT-blockchain-based model for the remote patient monitoring* is proposed, with the higher level of the security and privacy. This higher level of protection is achieved through the use of various elements, including advanced, cryptographic techniques such as lightweight one, like ARX encryption scheme, ring signatures (with such significant privacy features as signers anonymity and signature correctness), double encryption scheme, *and Diffie-Hellman key exchange technique concept*. The latter serves to enable a public key (PK) protection against an attacker. The authors showed how the analysis is carried out in the smart contract and then based on the results of such analysis how a health alert event (transaction performed by the actor of the healthcare) is created. To be precise, the data is sent to the smart contract, *which is used as a verification link*: formatted information is analyzed in and by the smart contract along with the threshold value. Then the threshold value makes a decision whether the health reading is matching the normal standard health data type (the one that is considered as a normal in the system) or not [30]. If the health data transmitted is considered by the smart contract as normal, the sender may sign the transmission adding a digital signature after that overlay network sends a signal to the health provider. If the health data transmitted is considered by the smart contract as abnormal, the smart contract is going to make an event and sends an alert to the patient, overlay network, and cloud servers. The overlay network is used in this case only for storage of transmission alert. According to the authors of [30], this blockchain-based IoT model provides reliable data communication over the network (double encryption scheme to make the symmetric key more secure over the network) and storage over the cloud.

This work offers a good set of cryptographic protections. Instead of only one type of encryption technique, *both encryption schemes, symmetric and asymmetric, were used for different purposes*: ARX encryption algorithm (using a particular branch of the symmetric key, called ARX algorithms, to encrypt the data for blockchain. These algorithms are made up of the simple operations, addition, rotation, and XOR, and support lightweight encryption for small devices). A asymmetric algorithm is used for public key encryption.

The last but not least unique feature proposed by the authors is a combination of the methods used: they introduced a useful set of cryptographic means, including Diffie-Hellman key exchange technique, symmetric and asymmetric keys, ARX encryption algorithm, digital signature, ring signature. This compilation of the methods wasn't not found in the other works dedicated to the security in healthcare. The authors also proposed an implementation and usage of the overlay network: it was used for simplification of the transaction and controlling measurements. The function of it is to be aware of abnormal operations and send alerts and notifications to healthcare providers. The omission in this part is that they mentioned only providers, but not all interested parties.

Moreover, a sound scheme of cryptographic protection with the participation of the overlay network is given. *The authors also highlighted two different overlay network functions depending on whether the data is normal or abnormal.* However, overlay network is used only for storage of transmission alert. In addition, a term *health alert event* has been introduced. Health alert events should also be anonymous and privacy preserved to the overlay network. This alert interpreted as a transaction made by a separate user, and in order to increase the level of security on the health information transferred, the alert may embrace all advance cryptographic techniques with the use of a new algorithm proposed by these authors. One other positive moment is that they highlighted the sender, receiver, and network functions (where the entity who is sending the information could be treated as a sender and the entity who is receiving the information could be treated as a receiver).

However, in spite of massive advantages of the work, it has a few omissions: the entire system is offered only for remote patient monitoring, and this is only a small part of the medical services that can be provided. In addition, for some reason, they call data "readings", which narrows the transmitted information and does not give a full picture of the data transmission in IoHT.

3.3 Successful Implementation of the Blockchain and Smart Contracts for Secure HER Sharing in E-Healthcare

In [45], the researchers based their progressive blockchain-based model on the Ethereum platform and made a suggestion that this technology is the best for the purposes of the healthcare sector's security and privacy assurance, since their EHR sharing blockchain-based architecture with the use of decentralized storage interplanetary file system (IPFS) demonstrated a higher level of protection for e-health (during evaluation of performance metrics and analysis) against external attacks.

The authors demonstrated the advantages of the Ethereum platform for providing security and privacy for the healthcare system. This was illustrated in the example of the *mobile cloud blockchain system*; therefore, it is beneficial for the future development of the telemedicine and remote patient control. It implemented *the order of access to medical data* (*EHR access*) *in the mobile application*, without having missed the user registration phase. However, it missed other important phases that were mentioned and analyzed in many other works, some of which will be discussed below.

Experiments have shown that *their system provides a higher level of security and privacy indicators such as flexibility, availability, decentralized access, identity management, user authentication, integrity, and data privacy*. The important thing is that they, unlike many, have emphasized the data privacy. On the other hand, despite the fact that the authors mentioned that in the Ethereum blockchain the *smart contract is an account that consists of data and code with multiple programmable functions*, they didn't indicate the functions which smart contract may carry out. However, it was mentioned that *functions defined in the smart contract can be triggered by a new transaction sent from an account of an actor*, in order to transmit data, handle the request, and handle an access management. This refers to the functions of smart contracts and helps to further develop the idea of using smart contracts for each type of data transfer transaction separately.

The omission of the work is that the healthcare provider is shown in a very narrow sense, even the hospital is not mentioned as a unit of medical care; however, the hospital is shown also as an actor, which manipulates medical data separately from the specialists working in it, and this is the positive aspect, because it refers to a smart hospital in its theoretical idea. Moreover, the admin and HER manager were added into the smart hospital scheme: there are two centralized authorities, where HER manager receives data from all patients and then stores data.

The other advantage is that this work highlights the fact that data on patients can be of two types: personal information and medical data. The significant advantage of the work [45] *is the division into an area* (*in the meaning of the location*), for example, rooms, surgery area, and so on, which allows for systematization of the data coming from patients belonging to the same group (area), while each area has its own ID, which was taken into account by authors when constructing the *data block structure of cloud EHR storage system* (to access a specific group of data in the blockchain). *At the same time, an e-health record itself acts as one of the areas*. It is beneficial that they separated a policy storage as a tool and even *created a separate base for policies, and this is an important addition to their structure, as well as recognition of the importance of policies*. However, the meaning of the policies (policy list) is more related to an access control system: *a peer in the blockchain* (*healthcare provider or patient*) *may accept some policy that reflects their relation in medical services* (when the access to the EHRs of the patient has only a specific doctor). *The policy list contains smart contracts of all actors for identification and further access control*, when the smart contract performs a new operation. The authors separated and described the *following functionalities of the smart contracts within created scheme*: access control (new scheme proposed), data offloading, data sharing (including data updating, data return, data request, record hash value), verification, user registration form with Ethereum account, EHR access results of an authorized user, transaction record of authorized EHR access, EHR result of an unauthorized user, and transaction record of unauthorized EHR access.

The authors showed the enormous potential of the blockchain and the functionality of smart contracts for the e-health industry: a detailed and profound experiment with assessing changes in the security level was carried out, a special architecture for medical records sharing was developed with the inclusion of various types of smart contracts, new actors, and types of transactions.

3.4 Health Records Authorization Process with the Implementation of the Permissioned Blockchain and Smart Contracts: ABAC as an Important Tool for Smart Healthcare

The researchers proposed in [39] their model of the authorization process of EHR with the use of the permissioned blockchain and smart contracts technologies and *with the attribute-based access control* (*ABAC*) *model* for improvement of the existing authorization model for manipulations with EHR and other medical data and enhancing the privacy and security characteristics of them. The Hyperledger Fabric platform, which has many useful built-in features, was implemented into this new scheme. This means that, first, in permissioned blockchain, all peers have to be *registered by a special authority – the Membership Service Provider* (*MSP*) [80, 81] – and, second, due to the fact that this type of the blockchain allows the use of ABAC which is directly built into the code of the smart contract [80], the smart contract ought to be altered every time when the ABAC rules need to be modified, which leads *to a permanent redistribution of the smart contracts and consequently to the more secure tamper-evident and distributed access control model suited toward use cases that require privacy*. The paper [39] also highlights the importance of using policies; however, the policies are not included in the scheme presented in the work. *The ABAC and role-based access control (RBAC) models both rely on a policy-driven implementation*. At the same time, a description is given of the advantage of the ABAC access system: the authors claim that this particular technology *is suitable for the healthcare system*, because it is supported by the Hyperledger Fabric (HF), which was originally created as a *foundation layer* to transport enterprise-grade blockchain platform that has a built-in element to support confidentiality and privacy of each possible customized model of the blockchain usage for different types of areas. This special feature of the HF is achieved due to the implementation of the transport layer security (TLS), channels, and private transactions. And this means that ABAC which uses HF benefits from its features.

The other noteworthy idea offered in [39] is an introduction of the PatientEHR as a type of smart contract. It is a benefit of this work since it is applicable specifically to this category of data (EHR of the patient). The functionality of the smart contracts is also presented by the authors: patient's record can be created, viewed, and updated with the PatientEHR smart contract. On the other hand, there are no other types of smart contracts mentioned or described; moreover, the work is generally and primarily related to the access control and EHR. Other types of data are not considered. Accordingly, many other functions of the smart contracts and the blockchain are not given, and there are much more of them than to provide and delimit access to EHR.

3.5 Extended Usage of the Smart Contracts: Functionalities of Smart Contracts

The work [17] is related mainly to the remote monitoring of the patient using Ethereum platform; however, this work contains the best list of the smart contracts functionalities offered by the authors who proposed the blockchain network and smart contracts technology for healthcare system: remote healthcare system (RHS) smart contracts and paradigm of smart devices (with the special processing mechanism for them). The researchers illustrated the processes of the initialization of each RHS smart contract and execution of each smart contracts function for three separated types of actors: healthcare provider (hospital), healthcare professional (doctors), and the main group – the patients. The authors offered various types of smart contracts (here – "SC") to perform different functions, namely, remote healthcare system SC, registration SC (doctor registration and patient registration), authorization SC, monitoring patient SC (or health monitoring system SC), and check patient SC included into the proposed blockchain network. It is a prospective proposal that deserves further consideration and development. These are the only authors who, in addition to patient monitoring, have highlighted such function of the SC as a check patient, and this function allows to not only analyze a patient's data but also control their health in the real time and react quickly using the ability of the smart contracts.

Moreover, other significant algorithm shown by the researchers is the processing mechanism of the medical devices to accumulate and assess parameters of the collected medical data which is used to define a normal and abnormal data from patient's sensors (consequently the data that indicate the normal and abnormal state of the patient's health's parameters) after evaluation of the data recording time on the smart contract. The mechanism sends proper activation or alert signals to the doctors or does nothing in case of lack of emergency. One of the main advantages of the work [17] is the proposed detailed verification of the smart contracts mechanism with implementation of the execution of the *remote healthcare system smart contract* for the security purposes. This verification scheme is able to demonstrate the absence of the hackers to intervene into the functions of the smart contracts if all functions of the developed smart contract within a period of the registration of actors and data exchange smart contracts were operating in due course. Thus, it was proved that the proposed model is effective against hackers.

Furthermore, the authors carried out an analysis *of the blockchain-based remote healthcare system and the non-blockchain-based remote healthcare system* and showed advantages of the former.

On the other hand, although the authors claim that in order to understand clearly how their system works, they explored the use of smart contract for each participant; among the participants, only healthcare providers (only hospitals) and healthcare professionals (only doctors) are distinguished, without an implementation of some other actors and service providers.

3.6 GDPR Insight: Combination of GDPR and Blockchain

The work [34] concentrated on the data privacy in IoT applications and compliance with the GDPR with the use of the blockchain technology and smart contracts *for helping users to control the access and possession of their medical data*. These control measurements require the consent from users before any data manipulation is performed by cloud-hosted services or smart medical devices. The blockchain is seen as an instrument of more safe tracking transmission of the personal medical data by the IoMT device due to the fact that the *blockchain network is more auditable in terms of actor's actions and their identity verification*. The researchers offered the model which includes *three smart contracts automated verification* undertook by IoMT devices on patients' medical and other data and which can enable a GDPR observance. The tests performed using Ropsten testing network showed that the direct connection exists *between the fee paid by the patient (user) and the amount of violations of the GDPR found*. It was also offered a combined method to automatically verify GDPR rules on data processing units with the purpose to verify GDPR compliance for IoT devices at design time and with the use of *combination of GDPR and the blockchain*. The main goal of this work was to illustrate the business processes and its components for a number of IoT devices using blockchain-based virtual machine (VM). The focus of this work is mainly on the smart devices and improvement of the privacy of data collected by such IoT devices from unauthorized persons, including miners.

Three types of the smart contracts proposed by the authors for verification of the GDPR compliance are the following: *privacy contracts* (stand for privacy policy and user consent), *submission contracts* (one which has a log function to send an information to the blockchain and what has a process name, a device's address, as well as information regarding blockchain-related activities: executed activity on user data, the personal data that has been processed by such activity, and the encryption status of this activity in the blockchain, which was deployed by a container for storage purposes) [34], and *verification contracts*, where verification contract may call both privacy and submission smart contracts.

Verification cost and intrusion detection is the other idea offered: This mechanism for determining the insertion of the GDPR compliance into the blockchain ecosystem is well shown. The functionality and purpose, as well as the limitations for full nodes and lightweight nodes when working on a blockchain platform, were well shown. The whole verification scheme is shown using blockchain exactly as a business process, which is also important for the healthcare system, where there are many actors who provide paid services.

Moreover, a formal model (following the privacy-by-design approach) is proposed for supporting GDPR compliance checking for smart devices. The authors proved that the more actors participate in the operation, the more *gas consumption* shall be expected. "Gas" is the "currency" (payment method) used in blockchain system to make any transaction. This forces further research in the field and sets tasks for the future in order to reduce gas consumption and reduce the cost of transferring data as well as determine (and then control) the budget to allocate to support compliance checking.

The classification of actors according to the GDPR (a data subject, a data controller or joint controller, and a data processor) was given; however, the authors did not bind (allocate) them to the actual actors in IoHT. These three types of actors are classified by their functionality: how they perform the verification function. It may be seen as a drawback, because for sure the verification function is not the only one that can be used to provide a privacy and security protection and assurance using smart contracts. The main omission of this research is that it focuses on data collected from smart medical devices; other types of data are not considered, despite the fact that there are still EHR, databases, and other elements of the IoMT ecosystem. The work focuses in detail on GDPR compliance, what led to abandonment of other legal and regulatory acts related to control in healthcare; however, this approach and the mechanism may be useful to create the same compliance system with blockchain implementation for the other legislation or standard compliance (take it as an example for development).

3.7 Healthcare Data-Trading Market Based on Blockchain

In the work [18], the researchers showed how secure and trusted patient-centric, transparent, and secure data sharing in IoHT network can be reached using the integration of the blockchain and theory of games. The authors emphasized that in healthcare sector medical devices traditionally interact with centralized cloud-based server, because the network is usually limited by only one health institution, and these institutions cannot share the personal health data (PHD) to such third parties as providers, cloud, and other IT service providers and various analytics without a patient's consent. In the IoT era, this is inappropriate to have such boundaries and obstacles; it is significant to collect and implement all actors and devices/equipment of the IoHT ecosystem and provide the secure data sharing in it, so that the patients can give their consent and all participants of IoHT can interact freely.

However, a model offered in the work [18] also has many advantages which may benefit the IoHT: they introduced an evolutionary game theoretic scheme so that it is possible *to find out the impact of verification on the level of trust within the various actors of the health data-trading system*. Therefore, this theory combines research on trust and theory of games with the main goal to detect and eliminate untrustworthy players from the interactions and operations. As one of the advantages of using blockchain, the authors indicate a practical and trustworthy data-trading application of the proposed model aimed to build a healthcare data-trading market for patients, hospitals, and researchers based on the blockchain platform PHD-trading system, which collects multiple local consortium blockchain platforms distributed geographically and near the source of data.

The authors used in their work the term personal health data (PHD) that is less succinct than the term EHR, but more detailed and focused on personal data and therefore more privacy-oriented. *The main idea of the paper* is to show how effectively to manage the health data. *The main advantage is the system of rewards the researchers proposed*: when patients receive them (rewards) in the form of tokens (in the form of health tokens in case they accomplished any improvement in terms of their health) *for sharing at their own risk their data with third parties, involved in this PHD-trading system*. That is, in fact, patients are given a wide range of powers. But at the same time, this is also a minus, since patients may not always understand which data is private, which is not, which data must be transferred to improve health, and which is not. Thus, it is clear that this work says more about the healthcare market, and not about security and privacy, which is also a disadvantage of this work, since in addition to the market value of patient data, these data have other values (for the health and safety of the patient).

An excellent scheme supporting functionality of the healthcare ecosystem was proposed by the authors which includes such actors as data requestors, sealers, and patients; however, it does not embrace all possible actors involved in providing healthcare services. The term "data requestors" includes a lot; however, it is not really specific and there is no direct list of actors in it (there is only an example of a pharmaceutical company and what data can be requested and for what). "Health authority" is not quite an intelligible term, especially within the framework of IoT, since it can be some kind of government agency and at the same time it can also be a private clinic (i.e., separation is required here). *These health authorities in the blockchain-based trading system are considered as managers for the sealers* who administer each transaction on the blockchain, for example, management of the trading-related transactions, access control policies, the shared data processing, as well as supplying closer computing and AI services [18]. One of the benefits of health authority is the support of the high-speed interaction between users (patient and all other entities) with low computational burden. The term "patient" also includes a medical device (IoT wearable medical device) – this is not entirely true, since a device can be implantable. Moreover, a medical device should be highlighted as a separate tool. The interesting fact is that in the paper the researchers were also introduced as one additional actor, as authors claim that data is being collected for further research in order to improve the healthcare system in the future.

3.8 Blockchain-Based Healthcare Monitoring Architecture

The authors of [43] also took into account such a mandatory system in the field of medicine as the *life monitoring system*, to which employees of a medical institution have access. This is a system for remote monitoring of the patient and their condition by medical staff, which uses wearable and other home sensors to establish health parameters of a patient's health state with the accumulation of all data in remote database. Hence, the architecture proposed in this work (healthcare monitoring architecture), respectively, consists of two components: *medical devices blockchain and consultation blockchain*. The allocation of the monitoring and control system into a separate segment is *important novelty*, since with the growth of telemedicine, such technologies and architectures will be developed and be implemented, and, accordingly, their security must be taken into account and ensured without fail. It is also significant that the live monitoring system is highlighted; this paper is the only one that paid attention to this type of instrument. However, this system can also be connected to implantable medical devices (IMD) and wearable IoMT devices and, therefore, the fact that the authors did not mention this, at least briefly, is a disadvantage of this work.

The positive aspect of the presented new healthcare monitoring architecture [10] is that it introduces two important types of blockchain: medical devices blockchain and consultation blockchain that collaborate to some specific extent with patient, medical device, and health workers and support the monitoring system with the data collected in order to compare the health data of the patient and, thus, react faster.

However, the proposed architecture covers only telemedicine and identifies only three actors (health worker, patient, and hospital), without specifying what the concept of "health worker" includes, but it shows that this health worker is the main actor in this framework. On the other side, the proposed architecture may be used for development of further IoT-blockchain-based schemes which will include all possible scenarios and actors.

3.9 IoT-Blockchain Ecosystem: Combination of Blockchain and Swarm Exchange Techniques

In the study [22], the researchers offered an electronic health record servicing scheme in IoT-blockchain ecosystem (BIoTHR) for secure and reliable patients or other health data transmission in the IoT *network using a private blockchain platform in combination with the swarm exchange techniques*. The latter is designed on top of the underlying blockchain-IoT layer and aimed to empower the security and privacy of IoHT ecosystem. The transmission performed through secured swarm nodes of peer-to-peer interactions with the implementation of the autonomous encryption-decryption methods *accomplished with the timely monitoring of health data transferred via IoT network*. The swarm exchange techniques associate security services to EHR blocks as well as employ a content-addressable network protocol *in order to transmit EHR in a safe manner*. Due to the immutability of the blockchain, medical data that is stored in blocks is secured in a way that also provides its privacy and integrity [82, 83]. One of the main characteristics of IoT, which is mentioned by the authors of [22] and other authors, as a challenging one, is a heterogeneity of the IoT and IoT sensors: *the blockchain and IoT solutions demand a constant reconciliation to match a heterogeneous norm of EHRs*. This fact can lead to the security and privacy problems [82, 84], because the majority of the data sources of EHRs consist of many structured and unstructured data types that may be considerably large (e.g., medical imagery), and consequently, it is difficult to transmit it safely *without additional security measures provided by the blockchain*. Thus, the researchers in [52, 82, 84] emphasized as well that healthcare sector, as one element of critical infrastructure, has a great demand for the security and privacy protection *regulations* (*requirements*) which have to involve privacy-aware authentication, data storage, integrity, secure transmission, tamper-proof monitoring, and other related issues.

The advantage of the work [22] is that various types of nodes are specially separated, depending on what they are responsible for (IoT body temperature node, IoT pulse rate node, IoT blood glucose sensor node, etc.). The benefit of this is that using the swam technique where many nodes communicate with one another in a clustered way in the blockchain ecosystem, all nodes will allow to increase the level of the exact health services (for each separate parameter of the health) as well as the level of the secure data transmission within a specific sector of the healthcare.

All in all, this led to a more transparent and safer HER and other medical data transmission.

Another important contribution of the work is that the authors presented a concept of “trusted” and “untrusted” parties that helps to develop an idea of trusted key list in the swarm node, which may be used by the patient or other actor to complete validation or other data exchange procedures in more secure manner, and, consequently, the entire environment will be considered as secured and trusted. The fact that this process complemented with the strict swarm exchange policy (what situated nearby and supply the process with straightforward exchange facilities and data transmission) makes the presented IoT ecosystem more reliable and resilient to attacks. However, the idea of the trusted parties wasn’t disclosed in detail within the framework of the introduced concept of trusted environment (e.g., patient, caregiver, doctor, medical professional, government agencies, and insurance organizations).

3.10 Blockchain-Based Database with Higher Level of Security Protection

The work [85] *generally* related to the creation of the database that can *in a secure manner gather any types of data during a clinical trial and then store it*, in secure way as well. *The blockchain framework* in the proposed scheme is used *as a network blockchain and as an external record management blockchain* and consists of the IoT, wearable medical devices (sensors), and computational power. *The external record management blockchain* is aimed to operate the data accumulated after visit of the patient to the doctor, and then it has to be added to the chain using the PoS algorithm that sets into action upon the consensus of all interested parties involved into providing health services. The primary goal of the *network blockchain* is to manage an online cloud storage where all, aggregated by the wearable device’s health records, are distributed and processed. This blockchain-based framework is proved to enhance the security, privacy, and efficiency of the data in the healthcare systems, since all data is processed in the blockchain nodes. Most importantly, *imagery* (medical imagery systems) and *prescription of the doctor* were singled out as a separate type of the EHR, while other papers do not contain this type of the data. The purpose of distinguishing two types of blockchain is to manage the data which is being generated during the patient’s visit to a doctor. It will help to provide a higher level of security protection of each type of the data.

The beneficial issue presented in the work is that the policy maker was singled out: this actor was mentioned and separated only in this work. That’s important, because the level of security and privacy in separate healthcare entity and in the whole healthcare infrastructure (industry) depends significantly on policy makers. The main work’s omission is that it is not shown in great detail how the proposed framework will operate; the authors presented only a general scheme that is not explained at all: how the elements of framework (actors, blockchain and cloud infrastructures, and so on) will all interact with each other, will it be possible to use a framework in case if cloud computing is unavailable (in general or at a certain moment), and how exactly the authors propose to increase the level of security.?

3.11 Information Diffusion Security Strengthening Using a Blockchain and Theory of Trusted Zones in Smart Medicine

In [24], innovative BC-based framework – *a blockchain decentralized interoperable trust (DIT) framework for IoT* **–** is introduced. This IoHT blockchain technology provides a paradigm shift *in securing ways of information diffusion.* The Ethereum and Ripple blockchain platforms were used for development of this framework in order to collect and associate the requests in the various *trusted zones of the IoHT*. The proposed framework claimed to ensure not only traditional features provided by the blockchain but also an ability to support secure and effective communications between nodes that could be further grown and handled in an efficient manner. The offered framework based on the Ethereum platform and Ripple blockchain that *manage a request over the trusted zones* improves the encryption and IoHT access control tools and provides the confidentiality and integrity of the health data using *IoT-based multi-cloud solutions* if data was compromised via advisory attacks.

The concept on trusted zones introduced shortly may be illustrated as follows: one zone relates to the patient, and the second one relates to the healthcare system. The trusted zone in the meaning of the research presented is the number of virtual members and primary objects (equipment and devices) that communicate using a health edge node and blockchain (namely, for this case, a Ripple chain) communication abilities, where members may vote on the transactions conformed by them. The omission there is that only the hospital and the laboratories (healthcare provider) and the patient have their own zone; other actors are not taken into account, in spite of the fact that in terms of security, these actors either must have their own trusted zones or they should be included into some of the available zones in order to safely transfer data. Otherwise, the security and privacy may be affected using these minor actors and their weaknesses. In fact, a new trusted zone is always created after the first request from any member so that operation can be validated by the blockchain. To join the trusted zone, every primary object (e.g., medical device) must execute a secure transaction. This concept of the authors of [24] is a prospective innovation offered which can be developed later.

Generally, DIT IoHT truly where a smart contract guarantees authentication of budgets and indirect trust inference system (ITIS) reduces semantic gaps and enhances trustworthy factor (TF) estimation via the network nodes and edges. In addition, different cases were explored (emergency case, notification case, and normal case); however, the smart contracts of different types of functionality for each case weren’t proposed or showed.

The drawback of the work is that the scenario on interconnections between few actors was illustrated, between patient, ambulance, and doctor (in the blood pressure sensor-ambulance-doctor-blockchain-health edge scheme). However, since the scenarios can be different and include not only these actors from the healthcare system, the idea is illustrated incompletely. An advantage that may be mentioned is that it describes the work of *the validation process*: if a new transaction is to be appended to the chain, all the participants in the network must approve (validate) this transaction. The researchers have made this by applying an algorithm that verifies the transaction (including two types of communication) and created for its implementation an algorithm of aggregation rules and association rules for smart contract zones. The problem here is in definition of the term "valid" by exact blockchain system, which may be different in the various blockchain networks.

The general particularity in this work is that actors (participants) were tied to nodes: between nodes (i.e., patients, healthcare providers, suppliers, etc.) on the healthcare IoT network. That is, not even the actors are listed or named, *but nodes act as users*, which are associated with different entities or persons.

3.12 Hyperledger Fabric Network Architecture with Introduction of Different Types of the Smart Contracts

The work in [19] focuses on securing electronic medical records (EMR) with the help of blockchain technology. Medical and personal data protection using the blockchain is also a prospective direction of the research, since there were and will be many attacks on medical records as it was pointed out in works [86]. In [19] the use of *three-tier application* (*front-end application, middleware APIs, Hyperledger Fabric Blockchain Network, MySQL database server*) *was proposed*.

The researchers offered in this work a term *intermediate solution provider*, but do not disclose it in their diagrams and descriptions, and this seems to be an oversight, since it is necessary that all possible third parties providing services should be taken into account in such diagrams. The hospitals and any intermediate solution provider have been added to Hyperledger Fabric Network Architecture proposed by authors. The offering of the group of the intermediate solution providers is a benefit of this work due to the fact that often information leaks through these intermediate actors, and the proposed separation also refers to the HIPAA rules.

The authors indicated that the database will be encrypted by the RSA algorithm, but it is not specified how the persons who serve these databases should act if the algorithm is overcome and the attacker gains access to the databases and how all parties should act, taking into account the requirements of HIPAA and other regulations and rules.

Since authors write that together all listed actors form a consortium blockchain network, there can be a new organization appended to the ecosystem – *which means* *that all new additions must also comply with regulatory purposes*. This is a positive part of the proposed scheme, since it offers the possibility of including new actors; however, it does not work out the details of such inclusion and expansion of the list of actors.

The authors used HF because it has a benefit: the certificate authority, which is built into Hyperledger Fabric, provides all actors with encryption keys and certificates. However, the advantage of it is *that it can be replaced with any other popular identity management services as Hyperledger Fabric supports pluggable CAs*. The benefit of the work [19] is that it perfectly distinguished various types of data (medical records, wearable data, medical history data, medication, lifestyle). Moreover, the authors explicitly pointed out that they used two main categories of actors – patient and healthcare provider, which develop the ideas behind HIPAA.

The main development made by the authors of [19] is an enlarged and detailed list of the functionality of the smart contracts, which is also illustrated at the schemes. There are such types of the smart contracts capacities as registration, login, upload data (upload patient record for the first time, updating new patient record), request data (including requesting patient data access, publish request using the blockchain nodes), respond to request (including fetch incoming patient requests), view data (including fetch provider request list), and revoke access (however, it is not shown how the smart contracts are used and which types of smart contracts exist in this group). Such advanced elaboration of functions of the smart contracts with the implementation into their scheme the idea of necessity to follow the rules (EU General Data Protection Regulation [GDPR] [63], Health Insurance Portability and Accountability Act of 1996 [HIPAA] [74], the European Union Medical Device Regulation of 2017 [EUMDR] [87]) *makes this work prospective for the future development*.

3.13 Key Agreement Protocol for IoMT Ecosystem Based on Blockchain

Offered by the authors of [37], Blockchain-Enabled Authenticated Key Management Protocol for Internet of Medical Things (BAKMP-IoMT) environment is mainly related to the IMD and secure transmission performed by these devices (IMD) for an end healthcare provider. The secure key management scheme presented in this research includes a transaction of the medical data from patient with IMDs to personal servers (e.g., smartphones) and then to the cloud servers where healthcare data resides in a safe manner due to the implementation of the blockchain technology into its work. Patient's data can be accessed by the user from the cloud server *after completing the strict steps of the user authentication process*. The cloud server in this model serves *as a blockchain-miner node of the IoMT* and is considered as a main storage of all medical data which supports the blockchain nodes. The formal security verification and security verification were performed by employing AVISPA, and the threat model was built after experiments.

As a result, the researchers proved that the proposed new BAKMP-IoMT model is resilient against IMD physical capture attack and the data modification attack at the cloud server, protects ephemeral secret leakage (ESL) attack, may resist replay attack, is able to protect against the man-in-the-middle attack (MITM), is able to protect privileged insider attack, and is secured against various impersonation attacks *as well as preserves anonymity and untraceability properties*. Consequently, it demonstrated higher security and functionality level in comparison with the other relevant models due to the sequencing of the stages of BAKMP-IoMT and the sufficiency of each stage and also due to the mechanisms that are embedded in each individual phase.

BAKMP-IoMT includes the following eight stages: (1) pre-deployment (this includes patient registration, IMD registration and cloud server registration), (2) key management (key management between a IMD and personal server; moreover, key management between a personal server and cloud server), (3) user registration, (4) login, (5) authentication and key agreement, (6) blockchain construction and addition, (7) password and biometric update, and (8) dynamic IMD addition (dynamic IMD addition, dynamic personal server addition, dynamic cloud server [miners] addition). *That is*, *in fact*, *more related to the* delineation of the blockchain's functionality; there is no more detailed list of smart contracts.

The main benefit of the work is that the profound threat model was created by the authors using few different methods – with implementation of few techniques such as Canetti and Krawczyk's adversary model (CK-adversary model) and the guidelines of widely used DY threat model. In addition, such actors as trusted authority and relative of patient were implemented into the framework proposed, and this trend is prone to cover more distant actors and it also has a great importance.

And last, but not least, involving a different scenario, the researchers showed and computationally proved that *the growth of number of devices and actors* (*IMDs and users*) *leads in all cases to more blocks in the blockchain while transmitting the data* (that's logical because new blocks are created if there are more data transmitted) and that *computational costs* augment in these cases as well.

The one significant advantage of this work is that the authors calculated every step and showed all the algorithms, a lot of cryptographic details, as well as that it was the *loading biometric data for user authorization* (*in addition to the password*) *highlighted* in the work.

The other one is that the authors showed differentiation of functionality of the blockchains, namely, patient registration, IMD registration, cloud server registration, user registration, and login phase; however, this is all without the implementation of the smart contracts into it, only the description of the blockchains was given, and it would be more advantageous if authors added some ideas regarding smart contracts.

3.14 Forensics-by-Design IoMT Authorization Using Blockchain and Smart Contracts

Forensics-by-design approach for securing healthcare management systems (*forensics-by-design framework for managing access to medical data and devices*) is presented in the work [42]. It is related mainly to *the IoMT authorization based on the blockchain and smart contracts*, *with integrity guarantees built in this system*. The blockchain and smart contracts technologies are used in this work to design an architecture which allows to create a *trust domain* and *then manage access control to medical data and medical devices*.

There were three features of the critical IoMT ecosystem singled out: the users' roles and capabilities, the interaction of users with the IoMT devices, and the access domain. The smart contracts were used to handle the authorization, perform and maintain system policies, and start transaction log integrity and privacy. For this purpose a new algorithm – *a consensus proof of medical stake* – was proposed in combination with the blockchain, the one which validates the operations, and the general focus was made on the medical devices and data it collects. *All the actors* (*stakeholders*) *are the clients of the offered blockchain architecture*. Using an Ethereum platform, users (actors) have an access to the data by linking the users to the health and technical data, respectively, via such unique identifiers *as Ethereum accounts of users and devices*. Appending such information and data enables potent storage and a comprehensive smart contract architecture, because this information (from the creation of data by the medical devices to its utilization) may be received through the functions implemented within the smart contracts.

The main drawback of this work is that the authors have proposed and tested their scheme and architecture in a theoretical ideal environment in which, as they imply, all attackers do not want to be penalized (there could be economic or reputational penalties, e.g., reputational risk may be presented as node's voting power [impact] is halved after any violation). However, in reality, not always everything corresponds to these specified ideal conditions. The great designation of this work is that in addition to the manufacturer as an entity, it also singled out manufacturer technicians – an actor rarely indicated in other papers. Clarifications on types of the medical devices are given many times in this work; it is even divided depending on their location (in patients' body or home or in hospital/clinic). Moreover, IoMT devices (medical devices like implantable, hospital devices, etc.), IPFS (interplanetary file system (IPFS) 2 protocol), and *treatment plan are listed as an important part of the IoHT environment in the work. End user is indicated as an untrusted domain with untrusted device*.

The main achievement is the distinction and detailed description of such types of functionalities of the smart contracts as registration smart contract (RSC), actor handling smart contract (AHSC), and log management smart contract (LMSC); these categories and its functional content are a significant contribution made by the authors into implementation of the smart contracts into smart medicine. The principal idea is that when calling a suitable corresponding function for registration, authorization, or managing logs, the user, the well-directed system based on blockchain technology, will perform these functions in more secure manner.

3.15 Blockchain for Medical Insurance

In [41], it was proposed to single out the healthcare insurance companies into a separate category of healthcare providers and to use the blockchain technology to protect information recorded for insurance purposes, since the authors rightly pointed out the need to integrate IoT and health insurance. The work mainly provides an overview of existing technologies based on the blockchain, applicable to IoT, primarily to IoHT. As one of the important points noted in [41], the use and implementation of the decentralized autonomous organizations (DAO) should be indicated in order to avoid the involvement of a third party to conduct transactions. *DAOs are an entity that is run through rules encoded as a smart contract, and their financial transaction record and program rules* are maintained on the blockchain. The smart asset company Digix is represented as token on the blockchain implementing *proof of provenance protocol.*

The researchers offered a good integration of blockchain and healthcare insurance. Moreover, the authors have written how smart contracts and the blockchain can benefit the healthcare insurance industry. Not in great detail this work indicated that *it can support automated claims, a transparent and reliable payment mechanism, and can be used to enforce contract-specific rules*; thus, due to this automation, a number of insurance operations will decrease that in turn results in the reduction of costs and time on insurance claims.

In general, the work has little connotation, and the solution of some problems, not to mention the results, is more focused on business goals rather than technical content. In the scheme proposed, there is no patient at all; however, the patient is an actor who gives a consent to the transfer of data to both the hospital and the insurer. Some functions of wearable devices are transmit and verify insurance claim – but this is only in the picture; the text does not say anything about it at all and this is an omission, since at least it was important to mention it. However, the work includes such functions of the blockchain *as a collection of the medical information and performance of a personal guidance.*

3.16 Summary

There is a plethora of research efforts devoted to many aspects, sometimes completely different, in many areas related to blockchain and smart contracts in smart healthcare, and many techniques have been proposed using blockchain, including mixed techniques. Some deserve attention and development, some can be integrated into existing mechanisms or schemes that will be created in the future, and some will be developed into something completely new, as yet unknown. Researchers worldwide have just begun to perform the investigations in this direction. All existing studies and published calculations, diagrams, and architectures have been published mainly in the last 2 years (from 2018 to 2022). However, despite this, the topic has been worked out quite seriously, and one challenge which has to be addressed in the future is the lack of synchronization of innovative proposals with existing or emerging standards and regulations in the field of the blockchain and smart contracts.

4 Concluding Remarks

In this chapter, the endeavor to give concise information about the use of blockchain and smart contracts in Smart Medicine 4.0 was made. After the relevant standards and research works related to the cyber-physical systems, Industry 4.0 and IoHT, were reviewed, it was established that it is necessary to consider new methods of improving the Smart Medicine 4.0 and providing security and privacy in the healthcare industry. Given that traditional measures to ensure information security and personal data protection are not sufficient for IoT devices and IoHT industry in general, due to their specific characteristics, such as limited storage, scalability, and heterogeneity of IoT devices and other features of IoHT studied out above, it may be proposed that the blockchain and smart contracts shall be implemented into the paradigm of the Smart Medicine 4.0. This way is beneficial and prospective, since it is the most appropriate new technique that combines all the qualities required to protect and support the medical sector and may be used with the implementation of various existing and new emerging methods and methodologies for protecting information security and personal data.

The main idea of this chapter is that the blockchain and smart contracts technologies are extremely promising for the medical field: many researchers, practitioners, and state agencies are working on their development and challenges. As mentioned above, the use of blockchain technology and smart contracts in healthcare is one of the priority areas for both theoretical understanding and comprehensive practical application. On the other hand, "*in the future, healthcare providers must expect new and more sophisticated attacks. Because healthcare providers provide critical services, they are more likely than others to pay the ransom to rebuild their systems as quickly as possible. This makes the sector an attractive target*" [86, 88, 89]. This means that the introduction of new methods of protection, which can resist more technically advanced hackers, is inevitable.

One thing is certain: the use of blockchain and smart contracts is one of the priority areas, and many authors consider these technologies as accelerators and precisely "blocks" for use in smart medicine, not only for data transmission, performing various technical and medical functions, but also for the improvement of the level of information security and, accordingly, the safety of patients. According to the author of this chapter, the directions in which the use of blockchain and smart contracts in principle and in smart medicine should develop are the invention and implementation of various types of smart contracts, each of which will be responsible for performing a clearly defined function in the smart medicine ecosystem, while all actors that will perform such operations will have their own tools, mechanisms, and roles for creating and using smart contracts.

Currently, smart medicine and everything related to it are under the control of government agencies and medical corporations [90], as well as agencies and companies involved in information security. The reason is clear: the smart medicine is the medicine of the future.

References

1. The European Union Blockchain Observatory and Forum, Blockchain applications in healthcare sector by EU blockchain. Blockchain-based Healthcare frameworks and ideas (2021). https://www.eublockchainforum.eu/sites/default/files/reports/eubof_healthcare_2022_FINAL_pdf.pdf. Retrieved March, 2022
2. European Parliamentary Research Service, Technological trends and developments. The latest updates from the ETH2 roadmap (2021). https://www.eublockchainforum.eu/sites/default/files/reports/March2022_Trends%20Report.pdf. Retrieved March, 2022
3. R.M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, K.K.R. Choo, Integrating privacy enhancing techniques into blockchains using sidechains, in *IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (2019), pp. 1–4
4. Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission DG Justice, Freedom and Security (2010). https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-130 the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf. Retrieved March, 2022
5. M. Hao, H. Li, X. Luo, G. Xu, H. Yang, S. Liu, Efficient and privacy-enhanced federated learning for industrial artificial intelligence. IEEE Trans. Ind. Inf. **16**(10), 6532–6542 (2019)
6. I. Kunz, P. Stephanow, C. Banse, An edge framework for the application of privacy enhancing technologies in IoT communications, in *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (2020), pp. 1–6
7. Y. Chen, X. Qin, J. Wang, C. Yu, W. Gao, Fedhealth: a federated transfer learning framework for wearable healthcare. IEEE Intell. Syst. **35**(4), 83–93 (2020)
8. A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, Fog computing for Healthcare 4.0 environment: opportunities and challenges. Comput. Electr. Eng. **72**, 1–13 (2018)
9. A. Aslam, E. Curry, A survey on object detection for the internet of multimedia things (IoMT) using deep learning and event-based middleware: approaches, challenges, and future directions. Image Vis. Comput. **106**, 104095 (2021)
10. G. Ioppolo, F. Vazquez, M.G. Hennerici, E. Andrès (2020). Medicine 4.0: new technologies as tools for a society 5.0. J. Clin. Med. **9**(7), 2198. https://doi.org/10.3390/jcm9072198U.
11. S. Palani, S. Mahesh, D. Vasanthi, D.S. Kumar, Ethereum blockchain based healthcare Industry ecosystem, in *2020 7th International Conference on Smart Structures and Systems (ICSSS)* (2020, July), pp. 1–5
12. S. Underwood, Blockchain beyond bitcoin. Commun. ACM **59**(11), 15–17 (2016)
13. S. Nakamoto, A. Bitcoin, A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf. Retrieved March 4, 2022
14. P. Hegedűs, Towards analyzing the complexity landscape of solidity based ethereum smart contracts. Technologies **7**(1), 6 (2019)
15. M. Pilkington, Blockchain technology: principles and applications, in *Research Handbook on Digital Transformations*, (Edward Elgar Publishing, Cheltenham, 2016)

16. G. Wood, Ethereum: a secure decentralised generalised transaction ledger, in *Ethereum Project Yellow Paper*, vol. 151 (2014), pp. 1–32
17. H.L. Pham, T.H. Tran, Y. Nakashima, A secure remote healthcare system for hospital using blockchain smart contract, in *2018 IEEE Globecom Workshops (GC Wkshps)* (2018), pp. 1–6
18. F. Alkurdi, I. Elgendi, K.S. Munasinghe, D. Sharma, A. Jamalipour, Blockchain in IoT security: a survey, in *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)* (2018, November), pp. 1–4
19. M. Parmar, S. Shah, Reinforcing security of medical data using blockchain, in *2019 International Conference on Intelligent Computing and Control Systems (ICCS)* (2019), pp.1233–1239
20. M.S. Urmila, B. Hariharan, R.A. Prabha, Comparative study of blockchain applications for enhancing internet of things Security, in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (2019), pp.1–7
21. M. Al Baqari, E. Barka, Biometric-based Blockchain EHR system (BBEHR), in *2020 International Wireless Communications and Mobile Computing (IWCMC)* (2020), pp. 2228–2234
22. P.P. Ray, B. Chowhan, N. Kumar, A. Almogren, BIoTHR: electronic health record servicing scheme in IoT-blockchain ecosystem. IEEE Internet Things J. **8**(13), 10857–10872 (2021)
23. J. Al-Jaroodi, N. Mohamed, Blockchain in industries: a survey. IEEE Access **7**, 36500–36515 (2019)
24. E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, O.Y. Song, A.K. Bashir, A.A. Abd El-Latif, DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access **8**, 111223–111238 (2020)
25. U.U. Uchibeke, K.A. Schneider, S.H. Kassani, R. Deters, Blockchain access control Ecosystem for Big Data security, in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (2018, July), pp. 1373–1378
26. Alphand O. et al., IoTChain: a blockchain security architecture for the Internet of Things, in *2018 IEEE Wireless Communications and Networking Conference (WCNC)* (2018, April), pp. 1–6
27. P. Tasatanattakool, C. Techapanupreeda, Blockchain: challenges and applications, in *2018 International Conference on Information Networking (ICOIN)* (2018), pp. 473–475
28. A. Rayes, S. Salam, *Internet of Things from Hype to Reality* (Springer, 2017)
29. S. Mishra, A.K. Tyagi, Intrusion detection in Internet of Things (IoTs) based applications using blockchain technology, in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (2019), pp. 123–128
30. G. Srivastava, J. Crichigno, S. Dhar, A light and secure healthcare blockchain for iot medical devices, in *IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)* (2019), pp. 1–5
31. M. Bakkar, A. Alazab, Information Security: definitions, threats and management in Dubai hospitals context, in *2019 Cybersecurity and Cyberforensics Conference (CCC)* (2019), pp. 152–159
32. L. Rachakonda, A.K. Bapatla, S.P. Mohanty, E. Kougianos, Sayopillow: blockchain-integrated privacy-assured IoMT framework for stress management considering sleeping habits. IEEE Trans. Consum. Electron. **67**(1), 20–29 (2020)
33. G.S. Aujla, A. Jindal, A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring. IEEE J. Sel. Areas Commun. **39**, 491–499 (2020)
34. M. Barati et al., GDPR compliance verification in internet of things. IEEE Access **8**, 119697–119709 (2020)
35. R. Akkaoui, X. Hei, W. Cheng, An evolutionary game-theoretic trust study of a blockchain-based personal health data sharing framework, in *2020 Information Communication Technologies Conference (ICTC)* (2020), pp. 277–281
36. J. Ranjith, K. Mahantesh, Privacy and security issues in smart health care, in *2019 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT)* (2019), pp. 378–383

37. N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J. Rodrigues, Y. Park, BAKMP-IoMT: design of blockchain enabled authenticated key management protocol for internet of medical things deployment. IEEE Access **8**, 95956–95977 (2020)
38. M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Blockchain leveraged task migration in body area sensor networks, in *2019 25th Asia-Pacific Conference on Communications (APCC)* (2019, November), pp. 177–184
39. R. Adlam, B. Haskins, A permissioned blockchain approach to the authorization process in electronic health records, in *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (2019), pp. 1–8
40. Y. Sun, F.P.W. Lo, B. Lo, Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access **7**, 183339–183355 (2019)
41. A. Karikari, L. Zhu, R. Dara, Blockchain: the next step in the development of the Internet of Things, in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (2018), pp. 341–345
42. V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, S. Katsikas, A forensics-by-design management framework for medical devices based on blockchain, in *2019 IEEE World Congress on Services (SERVICES)*, vol. 2642 (2019), pp. 35–40
43. O. Attia, I. Khoufi, A. Laouiti, C. Adjih, An IoT-blockchain architecture based on hyperledger framework for health care monitoring application, in *NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security, IEEE Computer Society* (2019), pp. 1–5
44. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: a blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J. **6**(5), 8770–8781 (2019)
45. D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access **7**, 66792–66806 (2019)
46. L. Luu, D. H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 254–269
47. X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, A.V. Vasilakos, Designing blockchain-based applications a case study for imported product traceability. Futur. Gener. Comput. Syst. **92**, 399–406 (2019)
48. K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, R. Wattenhofer, On scaling decentralized blockchains, in *International Conference on Financial Cryptography and Data Security* (Springer, Berlin, Heidelberg, 2016), pp. 106–125
49. M. Vukolić, The quest for scalable blockchain fabric: proof-of-work vs. BFT replication, in *International Workshop on Open Problems in Network Security*, (Springer, Cham, 2015), pp. 112–125
50. M. Bez, G. Fornari, T. Vardanega, The scalability challenge of ethereum: an initial quantitative analysis, in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)* (2019), pp. 167–176
51. E. Hildenbrandt, M. Saxena, N. Rodrigues, X. Zhu, P. Daian, D. Guth, G. Rosu, Kevm: a complete formal semantics of the ethereum virtual machine, in *2018 IEEE 31st Computer Security Foundations Symposium (CSF)* (2018), pp. 204–217
52. C. Hung, More healthcare data means growth for switch (2021). https://www.healthcareittoday.com/2021/02/17/more-healthcare-data-means-growth-for-switch/. Retrieved March, 2022
53. Reports and Data, Healthcare cybersecurity market to reach USD 27.10 billion by 2026 (2019). https://www.globenewswire.com/fr/news-release/2019/08/26/1906602/0/en/Healthcare-Cybersecurity-Market-To-Reach-USD-27-10-Billion-By-2026-Reports-And-Data.html. Retrieved March, 2022
54. S. Morgan, 2019 Cybersecurity almanac: 100 facts, figures, predictions and statistics, in *Cybercrime Magazine*, vol. 6 (2019)

55. J. Davis, 82% IoT devices of health providers, vendors targeted by cyberattacks (2019). https://healthitsecurity.com/news/82-iot-devices-of-health-providers-vendors-targeted-by-cyberattacks. Retrieved March, 2022
56. D. Joshi, How the laws and regulations affecting blockchain technology and cryptocurrencies, like Bitcoin, can impact its adoption (2021). https://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global. Retrieved March, 2022
57. U. K. J. Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (The LawTech Delivery Panel, 2019). https://technation.io/about-us/lawtech-panel. Retrieved March, 2022
58. J. Clayton, Chairman U. S. Testimony on "Virtual currencies: the oversight role of the US Securities and Exchange Commission and the US Commodity Futures Trading Commission" (2018). https://www.banking.senate.gov/imo/media/doc/Clayton%20Testimony%202-6-18.pdf. Retrieved March, 2022
59. Senate bill dated 20 of March 2017 N 398–Senator Kieckhefer, Establishes various provisions relating to the use of blockchain technology. (BDR 59–158) (2017). https://www.leg.state.nv.us/App/NELIS/REL/79th2017/Bill/5463/Text. Retrieved March, 2022
60. Chapter 97 House bill dated 29 of March 2017 N 2417, An act amending section 44-7003, Arizona revised statutes; amending title 44, chapter 26, Arizona revised statutes, by adding article 5; relating to electronic transactions (2017). https://www.azleg.gov/legtext/53leg/1R/laws/0097.pdf. Retrieved March, 2022
61. Act dated 2020 N 341 Regular Session House Bill N 701, On virtual cryptocurrency business (2020). http://www.legis.la.gov/legis/ViewDocument.aspx?d=1182592. Retrieved March, 2022
62. Blockchain 2019 Legislation (2019). https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2019-legislation.aspx. Retrieved March, 2022
63. General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu) (2016). https://gdpr-info.eu/. Retrieved March, 2022
64. Directive of the European Parliament and of the Council of 12 July 2002 N 2002/58/EC, Concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (2002). https://edps.europa.eu/sites/default/files/publication/dir_2002_58_en.pdf. Retrieved March, 2022
65. Directive of the European Parliament and of the Council dated 12 of August 2013 N 2013/40/EU, On attacks against information systems and replacing (2013). https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF. Retrieved March, 2022
66. Regulation of Cryptocurrency: Canada (2020). https://www.loc.gov/law/help/cryptocurrency/canada.php. Retrieved March, 2022
67. CSA Staff Notice 46-307 Cryptocurrency Offerings (2017). http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency_offerings.htm, https://perma.cc/7XF6-3T3E. Retrieved March, 2022
68. Canadian Securities Regulators Outline Securities Law Requirements that May Apply to Cryptocurrency Offerings: Press Release, CSA (2017). https://www.securities-administrators.ca/aboutcsa.aspx?id=1606, https://perma.cc/4KL4-YSEV. Retrieved March, 2022
69. C. O'Hara, OSC approves Canada's first blockchain ETF: the globe and mail (2018). https://www.theglobeandmail.com/globe-investor/funds-and-etfs/etfs/osc-approves-canadas-first-blockchain-etf/article37828183/, https://perma.cc/V6TD-KZ5C. Retrieved March, 2022
70. Blockchain and cryptocurrency regulation 2021. 12 legal issues surrounding the use of Smart contracts (2021). https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/12-legal-issues-surrounding-the-use-of-smart-contracts. Retrieved March, 2022
71. House bill N 1900 dated 9 of January 2019, A BILL to amend the Code of Virginia by adding in Article 6 of Chapter 2 of Title 2.2 a section numbered 2.2-214.2, relating to the Health Care Provider Credentialing Solution Fund; blockchain technology (2019). http://leg1.state.va.us/cgi-bin/legp504.exe?191+ful+HB1900. Retrieved March, 2022

72. House bill 19-1247 dated 30 of May 2019, An act concerning a study by the commissioner of agriculture on the potential applications for blockchain technology in agricultural operations (2019). http://leg.colorado.gov/sites/default/files/documents/2019A/bills/sl/2019a_sl_375.pdf. Retrieved March, 2022
73. Substitute House Bill dated 21 of March 2019 N 5417 of the House of Representatives, An act establishing a task force to study the use of blockchain technology to manage elector information (2019). https://www.cga.ct.gov/2019/FC/pdf/2019HB-05417-R000081-FC.PDF. Retrieved March, 2022
74. Health Insurance Portability and Accountability Act of 1996 (HIPAA) (1996). https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html. Retrieved March, 2022
75. A.M. Khattak, F. Iqbal, P.C. Hung, J.S. Sun, G.P. Pan, J.J. Lin, Privacy requirements for mobile e-Service in the Health Authority-Abu Dhabi (HAAD), in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (2016), pp. 204–209
76. European Union Agency for Network and Information Security, *Smart Hospitals Security and Resilience for Smart Health Service and Infrastructure* (2016). https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals. Retrieved March, 2022
77. European Union Agency for Network and Information Security, *Cloud Security for Healthcare Services* (European Union Agency For Network And Information Security, 2021). https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services. Retrieved March, 2022
78. European Union Agency for Network and Information Security, *Procurement Guidelines for Cybersecurity in Hospitals. Good Practices for the Security of Healthcare Services* (2020), https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services. Retrieved March, 2022
79. European Union Agency for Network and Information Security, *Security and Resilience in eHealth Security Challenges and Risks* (European Union Agency for Network and Information Security, 2015). https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services. Retrieved March, 2022
80. N. Emmadi, R. Vigneswaran, S. Kanchanapalli, L. Maddali, H. Narumanchi, Practical deployability of permissioned blockchains, in *International Conference on Business Information Systems* (Springer, Cham, 2018), pp. 229–243
81. C. Saraf, S. Sabadra, Blockchain platforms: a compendium, in *2018 IEEE International Conference on Innovative Research and Development (ICIRD)* (2018), pp. 1–6
82. V. Gatteschi, F. Lamberti, C.G. Demartini, C. Pranteda, V. Santamaria, To blockchain or not to blockchain: that is the question. IT Prof. **20**(2), 62–74 (2018)
83. D. Puthal, S.P. Mohanty, Proof of authentication: IoT-friendly blockchains. IEEE Potentials **38**(1), 26–29 (2018)
84. M.A. Sayeed, S.P. Mohanty, E. Kougianos, H. Zaveri, A fast and accurate approach for real-time seizure detection in the IoMT, in *2018 IEEE International Smart Cities Conference (ISC2)* (2018), pp. 1–5
85. M. Quasim, F. Algarni, A.A.E. Radwan, G.M.M. Alshmrani, A blockchain based secured healthcare framework, in *2020 International Conference on Computational Performance Evaluation (ComPE)* (2020), pp. 386–391
86. E. Doynikova, A. Polubaryeva, Analysis of the problems, their possible solutions and existing prospects of information security issues of wireless medical devices. in *Actual Challenges of Infotelecommunications in Science and Education, Collection of Scientific Articles: Materials of the IX International Conference on Advanced Infotelecommunications ICAIT, Volume 1 Plenary. Infocommunication Networks and Systems* (2020), pp. 419–424
87. ISO/IEC 62304:2006, Medical device software – software life cycle processes. https://www.iso.org/ru/standard/38421.html. Retrieved March, 2022
88. J. Davis, Maze ransomware hackers extorting providers, posting stolen health data (2020). https://healthitsecurity.com/news/maze-ransomware-hackers-extorting-providers-posting-stolen-health-data. Retrieved March, 2022

89. USA Food, Drug Administration, Cybersecurity in medical devices: quality system considerations and content of premarket submissions draft guidance for industry and Food and Drug Administration staff (2022). https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions?utm_medium=email&utm_source=govdelivery. Retrieved March, 2022
90. A. Levina, G. Ryaskin, S. Taranov, A. Polubaryeva, Effectiveness of using codes with a sparse check matrix for protection against algebraic manipulations, in *2021 International Conference Automatics and Informatics (ICAI)* (2021), pp. 292–295

Part IV
Blockchains and Currency

Post-Quantum Digital Signatures for Bitcoin

Miguel Ángel León-Chávez, Lucas Pandolfo Perin, and Francisco Rodríguez-Henríquez

1 Introduction

In 1982, Chaum introduced the concept of e-cash in [15] employing blind signatures allowing untraceable payment systems offering auditability and control and at the same time offering personal privacy. The e-cash, electronic money, electronic coin, or digital money tries to emulate its paper money counterpart in terms of functionality, i.e., it is a medium to exchange goods, it is a unit of measurement, and it stores a value. Since then, e-cash has added several properties to its definition, such as the following [37]: independence, security, privacy (anonymity), offline payment, transferability, divisibility, and untraceability. Many protocols were published [6, 37] in order to meet these properties. However, they all required a central authority (the Bank), responsible for minting the electronic coin and detecting double-spending.

In 2008, unknown author(s) under the pseudonym of Satoshi Nakamoto [34] published a seminal paper that resolves the previous problems in a distributed way through a peer-to-peer network, the Bitcoin protocol. According to Nakamoto, "the network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work (PoW), forming a record that cannot be changed

M. Á. León-Chávez (✉)
Computer Science Faculty, Benemérita Universidad Autónoma de Puebla, Puebla, México

L. P. Perin
Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE
e-mail: lucas.perin@tii.ae

F. Rodríguez-Henríquez
Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE

Computer Science Department, Cinvestav IPN, Mexico City, México
e-mail: francisco.rodriguez@tii.ae

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_11

without redoing the PoW." The successive linking of transaction blocks using PoW was called the blockchain. Today, this paper has originated more than 2000 cryptocurrencies worldwide uncountable works related to blockchain applications and alternatives to PoW consensus protocol.

Bitcoin utilizes two cryptographic algorithms: hash functions and digital signatures. In particular, it uses the SHA256 and RIPEMD160 as the hash functions and the Elliptic Curve Digital Signature Algorithm (ECDSA) based on the Koblitz curve secp256k1 parameters. ECDSA is based on the discrete logarithm problem (DLP) defined as follows: find a scalar $k \in \mathbb{F}_n$ from the equation $Q = [k]G$, where Q and G are two points on an elliptic curve secp256k1 defined over the prime field $\mathbb{F}_p$ by the equation, $y^2 = x^3 + 7$. Here p and n are two 256-bit prime numbers.

During the last 45 years, the DLP problem and the integer factorization problem (IFP) have been used as hard mathematical problems providing the security assumption foundations of modern cryptography. However, in 1994, Shor [45] published two polynomial-time algorithms for solving both the DLP and the IFP on a quantum computer. Therefore, once such large quantum computers become available, the security of all applications based on these problems will be vulnerable, e.g., RSA digital signature, Digital Signature Algorithm (DSA), and ECDSA, as shown in [1, 23, 39, 41]. Even more, in 1996, Grover [25] published a quantum algorithm to speed up database search. This algorithm could be directly adapted to weaken symmetric cryptographic algorithms, such as the hash functions employed by Bitcoin, possibly affecting the PoW protocol.

In the context of cryptocurrencies, some believe that the threat of quantum attacks can be partially mitigated by not disclosing the public keys and avoiding address reuse. While this might be true for newly created wallets, public keys inevitably have to be made public for authorization of transactions. At this point, there is a gap where quantum attacks are viable. According to [14], these gaps can occur while transactions are broadcast but are still pending validation by miners. Another possible scenario is the case where transactions fail to consolidate or get rejected due to insufficient funds, low fees, or any other reason. Malicious parties could benefit during the interval when the public key is made public and forge new transactions to hijack their funds by recovering the private key using a quantum computer. New cryptographic primitives are thus required to prevent these attacks such as the adoption of Post-Quantum Cryptography (PQC), i.e., algorithms that are quantum-resistant and classical-resistant simultaneously.

An additional argument in favor of the adoption of a post-quantum version of Bitcoin has to do with the high influence that reputation has on the price of the highly volatile cryptocurrencies. If large-scale quantum computers are available, it would arguably be public distrust on those cryptocurrencies still relying on classical cryptography.

On the other hand, in 2016, the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, worried about theoretical and practical advances of quantum computing, published an internal report on PQC (NISTIR 8105) claiming that some instances of RSA, DSA, and ECDSA could potentially be broken by as early as 2030. Consequently, NIST published a request for Public Key Post-Quantum Cryptographic Algorithms [35]. As an outcome, multiple candidates are expected to be standardized and added to the Digital Signature Standard (NIST 186-4) as well as recommendations for Pair-Wise Key Establishment Schemes, replacing DLP (NIST 800-56A) and IFP (NIST 800-56B).

From 82 initial candidates, 69 moved to the first round of the NIST PQC competition. In 2019, only 26 candidates advanced to the second round, consisting of 17 public key encryption and key establishment schemes and nine digital signatures schemes [36]. On July 22, 2020, NIST published the status report on the second-round candidates [2], and it announced three third-round finalists for digital signatures as well as three alternate candidate algorithms for standardization at the end of 2024.

The PQC digital signature candidates that reached the third round are Crystals-Dilithium, Falcon (Fast-Fourier Lattice-based Compact Signature over NTRU), and Rainbow. In addition, GeMSS (Great Multivariate Short Signature), Picnic, and SPHINCS+ are considered alternate candidates. These algorithms are based on problem assumptions that are difficult to solve using quantum and classical computers, as follows: Crystals-Dilithium and Falcon are lattice-based cryptographic schemes, whereas Rainbow and the alternate GeMSS are Multivariate-polynomial-based cryptographic. Picnic and SPHINCS+ are based on symmetric primitives and hash functions, respectively.

Moreover, the NIST status update on the third round [33] presented during the third NIST PQC standardization conference held on June 7–9, 2021, and NIST announced the following: (a) it expects to select at most one algorithm based on lattice for standardization. (b) Cryptanalytic results have created some concerns about the security of both multivariate schemes Rainbow and GeMSS. (c) There will be a new call for PQC digital signature scheme proposals, which are not based on structured lattices and target specific applications, for example, a scheme with very short signatures.

In [18], it was presented an extensive comparison of the characteristics and the performance of the most promising post-quantum public key encryption and digital signature schemes for blockchains. This chapter analyzes the post-quantum digital signature candidates accepted in the third round of the NIST competition as alternatives for Bitcoin and points out the challenges for their adoption. As presented in the following subsections, short signatures are not enough for applications such as Bitcoin, which also requires small public key sizes.

The outline of the remainder of the chapter is as follows: the related work is summarized in Sect. 2. Section 3 identifies the Bitcoin security requirements and constraints on the PQC digital signatures proposals. Section 4 gives a brief description of the NIST finalists and alternates. Section 5 presents the performance analysis of the classical and PQC digital signature algorithms. In Sect. 6, design challenges for adopting post-quantum solutions in Bitcoin are explained. Finally, the conclusions and the future research work are drawn in Sect. 7.

2 Related Work

In the context of the Bitcoin protocol, several proposals have been published to replace its ECDSA digital signature scheme using the Koblitz curve secp256k1 parameters. This section organizes the proposed solutions according to underlying mathematical problems that are difficult to solve using either quantum or classical computers as follows: lattice-based, hash-based, and multivariate-polynomial.

2.1 Lattice-Based

The authors of [21] proposed a post-quantum blockchain (PQB) based on the lattice short integer solution (SIS) problem. The authors use the lattice basis delegation algorithm to generate secret keys by selecting a random value and using preimage sampling algorithm to sign the messages. In addition, they design a double-signature defined as the first-signature and last-signature in the scheme to reduce the correlation between the message and the signature. The authors claim that the sizes of the signature and secret keys are relatively shorter than others published PQ digital signatures based on lattice but without application to the blockchain. The authors did not propose concrete parameters for their approach.

In [47], the authors propose an anti-quantum transaction authentication scheme in the blockchain. In this approach, the public and private keys are generated from a set of master public and private keys (Seed Key). The authors use the Bonsai Trees technology and propose a new authentication method to extend a lattice space to multiple lattice spaces accompanied by the corresponding key. The authors did not propose concrete parameters for their approach.

The authors of [31] also proposed a lattice-based signature using the Bonsai Trees technology. The authors did not propose concrete parameters for their approach.

In [11], the PQC digital signature algorithm qTESLA was proposed to be used in Bitcoin. The NIST candidate qTESLA reached the second round of the NIST competition. However, according to [2], it has a poor performance. The public key sizes of q-TESLA-p-I and q-TESLA-p-III are about 15 to 20 times as large as those of Falcon and Crystals-Dilithium, in addition to larger signature sizes as well. On the other hand, qTESLA is roughly 2 to 5 times slower than Falcon and Crystals-Dilithium. For these reasons, qTESLA did not advance to the third round.

The authors of [43] proposed the usage of Crystals-Dilithium, concluding its relevance for quantum secure blockchains.

2.2 *Hash-Based*

In [14], it was proposed a Blockchained PQ Signature (BPQS), which is a modified version of the hash-based XMSS scheme. BPQS provides a fallback mechanism to support many-time signatures. The authors present a performance analysis and conclude that it is computationally comparable to non-quantum schemes, in particular, to ECDSA. Nevertheless, the main drawback of this approach is that the size of its output signature increases linearly with the number of signatures.

In [46], it was presented the eXtended Naor-Yung Signature Scheme (XNYSS). This signature combines a hash-based one-time signature scheme with Naor-Yung chaining for creating chains of related signatures. The authors claim that their proposal achieves smaller signatures and better performance than other hash-based signatures, such as XMSS. Table 1 shows the signature size for the long-term signature using the security parameter ($n = 32$), the branching factor ($b = 3$), and Winternitz parameter ($w = 16$).

Both the Quantum-Resistant Ledger (QRL) [40] and the Bitcoin Post-Quantum [3] cryptocurrencies use the XMSS scheme. The cryptocurrency IOTA [19] employs the Winternitz one-time signature (W-OTS) and the Ed25519 digital signature to provide a security level of 128 bits.

In [42], the authors propose to use the Novel One-Time Signature (NOTS), which offers minimum key and signature sizes from all of the existing OTS schemes. According to the authors, using SHA256 as the Hash function NOTS achieves an 88% reduction in both key and signature sizes as compared to the popular WOTS scheme.

PQChain was proposed in [5] implementing a hash combiner ($\text{Comb}^{H_1 H_2}$) that combines two hash functions H_1 and H_2 such that a given hash function property (for example, collision resistance) is preserved as long as at least one of the hash functions H_1 or H_2 has that property. The authors propose combining SHA3 with other Hash functions to diversify the portfolio.

2.3 *Multivariate-Based*

In [44], the authors proposed an Ethereum post-quantum variant using Rainbow as its digital signature. The authors' approach requires a public key storage server storing both the public key and the address of each user. This mechanism was put in place because Rainbow's public key is considerably large. Hence, the transaction does not need to include the large key material; it only needs to include the short address generated from the public key. Verifying signatures requires that a node requests to the storage server the public key of the corresponding address. Hence, the solution in [44] becomes highly centralized. Table 1 shows the values for the security strength of 128 bits.

Table 1 Public key, secret key, and signature sizes (in Kilo bytes) for the post-quantum solutions proposed in the literature

Digital signature	Class	Public key	Secret key	Signature
Dilithium [43]	Lattice	1.3	–	2.4
AQTA [47]	Lattice	157.8	550.4	308
qTESLA-I [11]	Lattice	1.5	1.2	1.4
XNYSS [46]	Hash	–	–	2.3
NOTS [42]	Hash	1	1	1
Rainbow(21, 36, 22) [44]	Multivariate	136.1	101.5	0.079

Table 2 Bitcoin security and performance requirements

Security	Requirement	Bitcoin
Digital signature	128 bits	ECDSA-secp256k1
Private key length	256 bits	256 bits
Public key length	Small	64 bytes
Signature length	Small	64 bytes
Hash code length	Small	256 bits
Address length	Small	25–36 bytes
Block size	Small	1–4 MB
Key generation time	Offline	0.10 ms [14]
Signing time	Fast	0.34 ms [14]
Verification time	Fast	0.25 ms [14]

3 Bitcoin Security Requirements

This section describes Bitcoin security requirements and constraints regarding the security strength of its cryptographic algorithms, space, and time required for constructing the transaction blocks. Table 2 summarizes those main Bitcoin requirements, where the entries in bold indicate the constraints required for avoiding a hard fork.

In public key cryptography, each user owns a public/private key pair. The private key is only known by its owner, whereas the public key is known key by all the users in the system. The key pair is generated in such a way that knowledge of the public key and the signing/verifying algorithms does not permit to deduce the private key. At the same time, it is computationally easy to sign/verify the plaintext using the keys. A digital signature scheme has three main primitives: key generation, signing, and verification. In key generation, the signer generates his/her private and public keys. To sign a document, the signer typically first computes the hash of that document using his/her private key to produce its signature. Given the document that was signed, its corresponding signature, and signer's public key, any entity can accept/reject that signature.

Bitcoin [34] defines an electronic coin as a chain of digital signatures. "Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership."

3.1 Digital Signature Algorithm

Bitcoin specifies the usage of the ECDSA using the Koblitz curve secp256k1 [13] parameters providing a security strength of 128 bits, i.e., the number of operations required to break the algorithm is approximately 2^{128}. This same digital signature scheme is also used by other cryptocurrencies, including Ethereum, XRP, Dash, Litecoin, Zcash, EOS, TRON, Ripple, Byteball, and Tezos. The main reasons for the popularity of ECDSA among the cryptocurrencies are its small key sizes and the excellent performance of its signing and verifying processes.

The recommended parameters of the Koblitz curve sec256k1 are specified by the sixtuple $T = (p, a, b, G, n, h)$. The elliptic curve secp256k1 is defined by the equation $y^2 = x^3 + 7$ operating over the prime field $\mathbb{F}_p$, where p is the prime $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$. The base point G in compressed form is equal to $G = 0279BE667EF9DCBBAC\ 59F2815B16F81798$. The so-called group order n of the point G and the cofactor h are given as

$$\begin{aligned} n &= oXFFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFE \\ &\quad BAAEDCE6\ AF48A03B\ BFD25E8C\ D0364141: \\ h &= 01. \end{aligned}$$

Using these parameters, a user generates his/her key pair consisting of a private key integer k, which is randomly selected in the integer interval $[1, n]$, and a public key curve point computed as $Q = (x_Q, y_Q) = [k]G$.

Hence, the size of the private key is 256 bits, which can be represented as 32 bytes or 64 characters in hexadecimal, and the public key is a point on the curve (x_Q, y_Q) of size 512 bits ($x_Q = 256$ bits and $y_Q = 256$ bits). However, the public key can be compressed to 257 bits by replacing the y-coordinate of Q by a sign bit (see below). The signature is the pair point (r, s) of size 512 bits ($r = 256$ bits and $s = 256$ bits).

In Bitcoin, the public keys (in script) are given with a prefix $0x04$ followed by $\langle x \rangle\ \langle y \rangle$, where x and y are 32 byte big-endian integers representing the coordinates of a point on the curve or in compressed form given as $\langle \text{sign} \rangle\ \langle x \rangle$ where $\langle \text{sign} \rangle$ is $0x02$ if y is even and $0x03$ if y is odd. The signatures use DER encoding to pack the r and s components into a single byte stream.

The private key allows spending the electronic coin (Bitcoin, BTC) by signing a transaction from one Bitcoin wallet to another. Usually, the user never handles the private key; instead, he/she will use a seed phrase that encodes the same information as the private key. There are three private key formats: hierarchical deterministic (HD) wallet keys, Base58 wallet import, and mini private key. A single seed value generates many private keys and each corresponding public key for HD. The seed value, also named master extended key, consists of a 256-bit key and a 256-bit chain code, for 512 bits in total. Base58 import format is a way of encoding an ECDSA private key to make it easier to print and copy. The mini private key format allows encoding a private key with 30 bytes. This format is especially convenient for applications where space is critical, such as QR codes.

3.2 Hash Function

Bitcoin uses SHA256 and RIPEMD160 to generate the Main Hash and address derivation. The Main Hash is the double hash (dhash), i.e., dhash(a) = SHA256(SHA256(a)). Main hash is used in the following processes: Proof-of-Work for mining purposes, generation of the Merkle tree that accommodates the hashes of each one of the transactions included in the block, and as a mechanism for chaining the blocks included in the blockchain. A Bitcoin address is the hash of a public key and is derived as follows in the original protocol:

$$\begin{aligned}
\text{Version} &= 1 \text{ byte}\\
\text{Key hash} &= \text{RIPEMD160(SHA256(public key))}\\
\text{Checksum} &= \text{First 4 bytes of dhash}(Keyhash)\\
\text{Bitcoin Address} &= \text{Base58Encode(Key hash}||\text{Checksum)}.
\end{aligned}$$

Nevertheless, the Bitcoin Improvement Proposal (BIP) 142 specifies the following two addresses for segregate witness (segwit), a soft fork specified in BIP141: Pay-to-Witness-Public-Key-Hash (P2WPKH) and Pay-to-Witness-Script-Hash (P2WSH). The Key hash field is again 20 bytes for P2WPKH addresses and, due to multi-signature purposes, 32 bytes for P2WSH addresses. A new field of one-byte value between 0 and 16 is added to the previous format to take into account the witness program version.

The BIP141 defines a new structure, called witness, that is committed to blocks separately from the transaction Merkle tree. This structure contains data required to check the transaction validity, but it is not required to determine the transaction effects. In particular, scripts and signatures are moved into the witness. BIP141 also changes the restriction on the block size, from 1 MB up to 4 MB. It must be noted that this change avoided a hard fork in the Bitcoin blockchain, and at the time of its implementation, it was the subject of an intense debate.

Furthermore, this soft fork was accomplished with a new transaction digest algorithm for signature verification, specified in BIP143, to minimize redundant data hashing in verification and to cover the signature input value. Its main restriction is on the public key size, where only compressed public keys of 33 bytes are accepted in P2WPKH and P2WSH.

Table 2 summarizes the Bitcoin security requirements, where the entries in bold indicate the constraints that PQC digital signatures must meet to avoid a hard fork. In [14], ECDSA-secp256k1 was implemented on an octa-core Intel Core i7-7700HQ at 2.80 GHz and using the Bouncy Castle Crypto APIs v.2.1.1, release 1.59, 2017.

4 Post-Quantum Digital Signatures

Even if the integer factorization problem and the discrete logarithm problem are no longer secure to attacks from large-scale quantum computers, there are other computing problems believed to be hard to solve using either quantum or classical computers. These problems are classified in [8] as secret key cryptography, hash-based, lattice-based, multivariate-polynomial, and code-based.

Secret key cryptographic, such as the Advanced Encryption Algorithm (AES), is based on permutations and substitution boxes known as S-boxes, which appear difficult to tackle using quantum computers. For some time, it was assumed that Grover's quantum algorithm could be used either to reduce the security of any k-bit secret key block encryption algorithm or k-bit hash function from k bits to just k/2 bits. However, it turns out that Grover's algorithm does not seem to parallelize very well, so much, so that some researchers even doubt if an attack based on this algorithm will ever be efficiently implemented. Indeed, even under the most optimistic assumptions, it appears that the security level of AES could be reduced from 128 bits to about 97.19 bits in the most pessimistic scenario when using Grover's algorithm [22].

Lattice-based cryptographic schemes, such as NTRU, Crystals-Dilithium, and Falcon, are based on the difficulty of solving several related problems such as the shortest vector problem, the closest vector problem, and the shortest integer solution. Let n be linearly independent vectors b_i defined over R_n, and a lattice is defined as any linear combination with integer coefficients of such basis as in (1).

$$L(b_0, \ldots, b_{n-1}) = \sum_{i=0}^{n-1} x_i b_i : x_i \in \mathbb{Z}. \tag{1}$$

The shortest vector problem consists of finding the shortest vector in the lattice considering its Euclidean norm. The fastest known solution takes $2^{O(n)}$ time and space. There also exists a polynomial-space algorithm that takes $2^{O(nlog(n))}$ time. The lattice-based NIST candidate algorithms, such as Crystals-Dilithium and Falcon, exploit what is called structured lattice schemes, which allows them to achieve significant efficiency for signing and verifying at the price of potential losses of security that must still be explored.

Hash-based cryptographic schemes, such as SHA-2 and SHA-3, are based on the security properties of the hash functions, i.e., collision-resistant, preimage-resistant (one-way), and second preimage-resistant. Moreover, this scheme is considered quantum-safe because of the same reasons discussed above.

The idea of SPHINCS+ is to authenticate a large number of few-time signature (FTS) key pairs using an abstract data structure named hypertree. FTSs are signature schemes that allow a key pair to produce a small number of signatures, in the order of ten for the SPHINCS+ parameter sets. A (pseudo) random FTS key pair is chosen to sign each new message. The signature consists of the FTS signature and the authentication information for that FTS key pair.

Picnic is based on a zero-knowledge proof system and symmetric key primitives like hash functions and block ciphers algorithms.

Multivariate-polynomial cryptographic schemes, such as HFE^{v-}, Rainbow, and GeMSS, rely on the multivariate-polynomial problem over finite fields. The public key is the polynomial sequence $P_1, P_2, \ldots, P_{2b} \in \mathbb{F}_2[w_1, \ldots, w_{4b}]$, where b is the desired security level in bits, and where the $4b$ variables $w_1, \ldots, w_{4b}$ have coefficients in $\mathbb{F}_2$. Each polynomial is square-free of degree two, and it is represented as a sequence of $1 + 4b + \frac{4b(4b-1)}{2}$ bits. The public key is large, and it has $16b^3 + 4b^2 + 2b$ bits. However, the signature of a message is short, and it has only $6b$ bits, namely, the $4b$ bits of the variables $w_1, \ldots, w_{4b} \in \mathbb{F}_2$, and an $2b$-bit string r, satisfying (2).

$$H(r, m) = (P_1(w_1, \ldots, w_{4b}), \ldots, P_{2b}(w_1, \ldots, w_{4b}))), \tag{2}$$

where H is a standard hash function. The verification process is simple as it requires b^3 bit operations to evaluate the polynomials $P_1, \ldots, P_{2b}$. The main advantage of this crypto scheme is that the signature is small with respect to all the other NIST post-quantum candidates. The security of this scheme lies on the difficulty of finding the sequence $w_1, \ldots, w_{4b} \in \mathbb{F}_2$ such that the polynomials $P_1, \ldots, P_{2b}$ can be produced. Using a brute-force approach, the probability of finding such a sequence is 2^{-2b}. On the contrary, the signee takes advantage of a predefined structure for generating the polynomials. This problem is known as the Hidden Field Equation (HFE). It is possible that an attacker can also take advantage of this structure. In fact, a powerful attack taking advantage of the structure used by the NIST candidates Rainbow and GeMSS128 was recently published in [9].

Code-based cryptographic schemes, such as McEliece's hidden Goppa-code, is based on error correcting codes. A linear code $C[n, k]$ defined over $\mathbb{F}_q$, with $q = p^m$, p a prime, is a k-dimensional vector in the subspace $(\mathbb{F}_q)^n$. A code can be defined by a generating matrix $G \in (\mathbb{F}_q)^{k \times n}$ or by a parity verification matrix $H \in (\mathbb{F}_q)^{k \times n}$ with $r = n - k$ as,

$$\begin{aligned} C &= \{uG \in \mathbb{F}_q^n | u \in \mathbb{F}_q^n\} \text{ or} \\ C &= \{v \in \mathbb{F}_q^n | Hv^T \in 0^r\}, \end{aligned} \tag{3}$$

where $HG^T = 0$. A vector s is called a syndrome of v, if $Hv^T = s^T$.

Two codes are said to be equivalent if they differ by a permutation in the coordinates of their elements. Formally, a code C' generated by G' is equivalent to a code C generated by G if and only if $G' = SGP$ for some permutation matrix $P \in (\mathbb{F}_q)^{n \times n}$ and a singular matrix $S \in (\mathbb{F}_q)^{k \times k}$. The permutation matrix is used as a public key for signatures. After finding a syndrome that can be decoded with the message, an error correction vector is used as a signature along with a value taken from a random oracle. In order to verify a signature, the permutation matrix is multiplied with the signature, which is checked with the help of the random oracle value.

4.1 NIST PQC Digital Signature Finalists

NIST defined five security strength categories [35] as follows, listed in order of increasing strength:

Level 1: At least as hard to break as AES128 (exhaustive key search)
Level 2: At least as hard to break as SHA256 (collision search)
Level 3: At least as hard to break as AES192 (exhaustive key search)
Level 4: At least as hard to break as SHA384 (collision search)
Level 5: At least as hard to break as AES256 (exhaustive key search)

Table 3 summarizes the length in bytes of the public keys, private keys, and signatures associated with NIST third-round finalist and alternate schemes as reported by their authors. We stress that no scheme proposes the security level 4, i.e., resistance to collision search on a 384-bit hash function.

There are three NIST finalists digital signature schemes, Crystals-Dilithium, Falcon, and Rainbow.

Crystals-Dilithium [32] was designed to provide NIST security levels 2, 3, and 5. The secret key is a set of parameters, but the signer can store a 32-byte value and then re-deriving from this seed all the other elements of the secret key. The authors also proposed a Dilithium-AES variant that uses AES-256 in counter mode instead of SHAKE, to expand the matrix and masking vectors and to sample the secret polynomials.

Falcon (512, 1024) [38] was designed to provide security levels 1 and 5. The secret key consists of four polynomials, and their values are not reported in the third-round proposal, although these values are about three times as large as the signature. According to the authors, the secret key could be compressed down to a small PRNG seed of 32 bytes.

Rainbow [17] is based on the Oil–Vinegar signature scheme which is a class of multivariate public key cryptosystems. Rainbow is characterized by producing extremely small signatures and highly efficient signature and verification times. On the downside, the sizes of Rainbow public/private keys are considerably large. Moreover, Beullens published in [9] an important attack against Rainbow that seriously compromise its security guarantees.

Table 3 NIST finalists and alternates length in bytes of the public key (PK), private key (SK), and signature (S) as reported by the authors

	Digital signature schemes		Level 1	Level 2	Level 3	Level 5
Finalists	Crystals-Dilithium [32]	PK	–	1312	1952	2592
		SK	–	32	32	32
		S	–	2420	3293	4595
	Falcon (512, 1024) [38]	PK	897	–	–	1793
		SK	32	–	–	32
		S	666	–	–	1280
	Rainbow [17]	PK	158K	–	861K	1885K
		SK	101K	–	611K	1376K
		S	66	–	164	204
Alternates	Picnic2-FS [48]	PK	32	–	48	64
		SK	16	–	24	32
		S	13802	–	29750	54732
	SPHINCS (small) [28]	PK	32	–	48	64
		SK	64	–	96	128
		S	8080	–	17064	29792
	GeMSS128 [12]	PK	352K	–	1238K	3040K
		SK	13K	–	35K	72K
		S	33	–	53	75

There are three NIST Alternate digital signature schemes, Picnic, SPHINCS, and GeMMS128.

The authors of the Picnic scheme [48] propose the following three variants by varying the parameters of both the zero-knowledge protocol used and the transformation that is applied:

Picnic-FS: uses ZKB++ with the Fiat–Shamir transform.
Picnic-UR: uses ZKB++ with the Unruh transform.
Picnic2-FS: uses a non-interactive zero-knowledge proof of knowledge with the Fiat–Shamir transform.

Table 3 only shows the Picnic2-FS variant for the security strengths 1, 3, and 5 because this variant provides the smallest signature length of the three ones listed above. We present in Table 3 the largest signature sizes reported by the authors. However, the authors also provide the average and the standard deviation of 100 Picnic signature sizes.

The authors of SPHINCS+ [28] propose parameter sets achieving security levels 1, 3, and 5; for each of these levels, they propose a size-optimized (ending on "s" for small) and a speed-optimized (ending on "f" for fast) variants. In Table 3, we only present the values corresponding for the size-optimized scheme.

According to the authors, the advantages and limitations of their proposal can be summarized in one sentence: "On the one hand, it is probably the most conservative design of a post-quantum signature scheme, on the other hand, it is rather inefficient in terms of signature size and speed."

GeMSS [12] is a multivariate public key cryptosystems that has key sizes and computational timings larger than the ones associated with Rainbow.

Even though NIST requested to test the submissions on a PQC Reference Platform, an Intel x64 running Windows or Linux and supporting GCC compiler, each author measured the computational efficiency on a distinct platform. Since each scheme was implemented on different CPUs at different frequencies, it is difficult to compare the timing computational complexity of the finalists and alternates. Fortunately, multiple research groups have developed platforms that allow to draw a fair comparison, as discussed in the next section.

5 PQC Digital Signatures Performance

Several research groups have implemented different tools and platforms that permit to have a fair evaluation of the NIST finalist and alternate digital signature schemes. The authors of [16, 27] present hardware and hardware/software co-design testbeds for comparing the performance of the candidate schemes. Software libraries executing on multiple platforms have been reported in [4, 7, 29, 30]. In this section, we present the timing performance reported in [7], as briefly explained next.

ECRYT Benchmarking of Asymmetric Systems (eBATS) [7] is a project that reports the performance of many public key schemes. It is based on SUPERCOP, a toolkit conceived for independently measuring the performance of cryptographic software using multiple CPU architectures and multiple computers, ranking from 1 up to 64 CPU cores at different frequencies. Concerning public key signature algorithms, eBATS measures the performance of cryptographic schemes based on the following main criteria:

- Time (in clock cycles) to generate a key pair
- time to sign a short message (59 bytes length)
- time to open a signed short message, i.e., verify a (larger) signed message and recover the original short message

In Table 4, we present a performance comparison of all the NIST finalists and alternate digital signature schemes. The timings of the finalist and alternates are given as reported in [7] when signing and verifying processes of 59 bytes on an AMD EPYC 7742: 64X2250 MHZ processor. Furthermore, we normalize these timings with respect to classical ECC curve P-256 timings. Following [7, 26], we have assumed that ECC key generation and signature require approximately 73,000 clock cycles, whereas verification takes about 200,000 clock cycles.

From a close observation of Table 4, note that none of the alternate candidates represent an option for being used in Bitcoin. They are problematic in terms of the sizes of the public keys, signatures, and/or because of their timing performances.

Table 4 Summary of the size and computational timings associated with all NIST finalists and alternates compared to classical ECC curve P-256 timings. Following [7, 26], we have assumed that ECC key generation and signature require approximately 73,000 clock cycles, whereas verification takes about 200,000 clock cycles. The timings of the finalist and alternates are given as reported in [7] when signing and verifying processes of 59 bytes on an AMD EPYC 7742: 64X2250 MHZ processor

		Size (bytes)			Time with respect to ECC		
	Schemes	PrivK	PubK	Sig	KGen	Signing	Verif
Classical schemes	ECDSA-256	32	64	64	1.0	1.0	1.0
	RSA-2048	512	256	256	1000	25	0.2
NIST finalists	Dilithium-2	32	1312	2420	1	2.5	0.4
	Falcon-512dyn	32	897	666	195	7.6	0.3
	Rainbow 1 Classic	49000	58800	66	72	0.5	0.1
NIST Alternates	GeMSS128	13438	352190	33	778	9429	1.2
	Picnic2l1-FS	16	32	13802	0.1	1516	300
	SPHINCS-s	64	32	8080	588	10133	10

One can also see in Table 4 that Rainbow enjoys an excellent signature and verification timing performance. However, Rainbow has a humongous public key size, and it has recently suffered a devastating attack [9].

It is interesting to remark that a number of hash-based digital signatures have been used in several cryptocurrencies currently active. For example, Quantum-Resistant Ledger (QRL), Bitcoin Post-Quantum, and IOTA, all use hash-based digital signature algorithms, which although not standardized can resist quantum attacks. However, the size of the signature of hash-based schemes still constitutes a critical issue for their adoption.

We stress that the two lattice-based candidates, Dilithium-2 and Falcon, have a verification time performance that is even faster than ECC. Since verification is arguably the most critical operation for cryptocurrencies, we conclude that adopting these two schemes for a post-quantum version of Bitcoin would not present issues with respect to timing performance. The (considerably) larger size of Dilithium-2 and Falcon public keys and signatures still remains as a point of concern though. (See Sect. 6 for an extended discussion of this issue.)

6 Implementation Challenges

This section discusses the challenges for integrating post-quantum signatures in Bitcoin, mainly considering the running time performance of the post-quantum algorithms previously described and the space requirement of storing public keys and signatures to validate transactions in the blockchain.

6.1 Running Time Requirement

Keeping the throughput of the cryptocurrency, namely the number of transactions per second, stable is crucial for its wide adoption. Therefore, the computational cost of digital signatures and their verification must be efficient. Since miners must verify that all transactions are valid before reaching consensus and publishing a new block, signature verification running time is undoubtedly the highest priority requirement for the signature scheme. For example, the daily average number of transactions per block for Bitcoin can vary from approximately 800 to 2700.[1] If the verification of a single signature takes 100 ms, verifying the signature of all block transactions would require up to 4 and a half minutes. That corresponds to about half of the expected time to publish a new Bitcoin block in the case of Bitcoin.

Considering all the finalist candidates of the NIST competition, as shown in Table 4, signatures can be efficiently verified from 2.5 to 10 times faster than ECDSA. The signature verification performance degrades for the alternate candidates to the point of running 300 times slower than ECDSA, which is unacceptable.

Signatures are generally performed to sign transactions before they are broadcasted to the Bitcoin's memory pool. This task is performed independently by the users and does not require much running time performance as verification. Signatures are computed only once, whereas they are verified many times before being included in the blockchain. However, there are cases where signatures must be fast, for example, exchange brokers or payment applications that broadcast many transactions in a short period. It is perhaps not surprising that the Finalist candidates perform better in this category than the alternates, which can be up to 10,000 times slower than ECDSA. Compared to RSA, finalist candidates are faster at signing, indicating that these schemes can bring a better trade-off for signing and verifying running time. That is not necessarily the case for key generation, which can be relatively slower. Nevertheless, key generation is performed mostly offline and by the users. Slower performance should not impact as much as it does for signature verification, and all candidates are at least faster than RSA.

On this note, the biggest challenge of deploying finalist candidates regarding running time performance would be to support these algorithms in dedicated hardware and other types of embedded applications, where often resources are constrained. Luckily, there have been significant advances to implement lattice-based candidates in small devices, also due to their compact keys and signatures [24, 30].

[1] https://ycharts.com/indicators/bitcoin_average_transactions_per_block.

6.2 Space Requirement

The maximum block size is fixed in the Bitcoin blockchain and cannot exceed 4 MB. Therefore, considering the block size restriction and the current size of public keys and signatures of the NIST candidates, the adoption of post-quantum signatures significantly reduces the maximum number of transactions in a single block. The trivial solution would be to increase the maximum block size to the point where it can admit the same number of transactions per block, thus preserving the current Bitcoin average throughput of 5 transactions per second. However, as mentioned before, increasing the maximum block size is not generally agreed upon in the Bitcoin community, thus reaching an impasse.

Ruling out the alternate candidates due to their poor signing and verifying performance, it is clear that the lattice-based schemes are the optimal choices for consideration. Because public keys must also be included with the signatures to validate the transactions, Rainbow's huge public key makes it unsuitable in practice. Moreover, the recommendation of avoiding address reuse brings deeper concerns over adopting schemes with large public keys, as these keys must be stored to preserve the continuous validation of the entire blockchain.

More recently, Bitcoin has activated a new feature with BIP 340 that enables multi-signatures and signature aggregation to speed up the verification process while reducing space requirements for more complex transactions. According to [10], multi-signature schemes allow signers to sign a message jointly, generating a short signature. A verifier can efficiently verify this signature and assert whether all signers signed the message. Aggregated signatures is a similar technique, but signers can individually sign distinct messages and aggregate their signatures, producing a short signature for all messages. The authors propose a compact multi-signature scheme that also allows public key aggregation. However, the proposed scheme is not post-quantum-resistant.

Since there are no post-quantum signature schemes with short public keys and short signatures simultaneously, signature or key aggregation could be an exciting solution to reduce the impact on the transaction throughput. However, there are no efficient multi-signature or aggregation schemes for the lattice candidates in the current state of the literature.

6.3 Public Key Recovery

Cryptocurrencies have adopted a public key recovery mechanism to reduce space usage in the blockchain. It is possible to recover the ECDSA public key of the signer using the signature and the signed message. Doing so avoids repeating information in the transactions, and comparing the address field with the obtained public key can confirm the recovery process. Hence, the public key does not need to be stored in the transaction, reducing the total space used in a block.

Post-quantum signatures and public keys are much bigger than ECDSA. Hence, a public key recovery method can further improve space requirements for their adoption. One example is the Falcon signature scheme that allows a public key recovery mode by including additional information in the signature [20]. As a result, the size of a signature increases by a factor of two, and the public key becomes a hash output. Recall that the hash of the public key corresponds to the address field that is already present in the transaction. The authors describe the *Key Recovery Mode* of Falcon in the updated version of their official specification.[2] Although they do not include it as part of the standardization process, it can reduce the total size of the signature with the public key by about 15%.

7 Conclusions

The DLP and the IFP have been the security assumptions of modern cryptography during the last 45 years. These assumptions will no longer be secure with the arrival of large-scale quantum computers in the near future. Bitcoin and other blockchains utilize the ECDSA signature scheme instantiated with the Koblitz curve secp256k1. This curve was selected because it achieves a high timing performance, which in turn imposes hard constraints on any substitution proposal of the NIST competition, including the post-quantum digital signatures Crystals-Dilithium and Falcon.

This chapter discusses challenges to deploying post-quantum signatures into cryptocurrencies. The running time performance of finalist post-quantum signature schemes of the third round of the NIST competition is satisfactory. Furthermore, optimizations can speed up the verification process, which is critical for keeping the network throughput, given that miners usually have state-of-the-technology computational power. However, considering the current maximum block size of Bitcoin, the size of public keys and signatures negatively affects the number of transactions per block. As a result, the number of transactions per second in the network will diminish, or the space required for storing public keys and signatures in the blockchain will grow. In this regard, the lattice-based candidates appear to be the most suitable candidates for deployment with cryptocurrencies. In addition, alternatives that further optimize space in the blockchain, i.e., multi-signatures or signature and key aggregation, are still an open problem in the post-quantum scenario.

Meanwhile, NIST recently announced a new call for post-quantum signatures considering unstructured lattices and targeting specific applications. In conclusion, the next NIST call for post-quantum signature schemes should consider such properties, in addition to the running time performance, such that applications like Bitcoin can take advantage of features that reduce space requirements. Also, new alternatives for storing public keys and signature scripts in the blockchain that minimize the inevitable impact of larger post-quantum signatures should be considered.

[2] https://falcon-sign.info/falcon.pdf.

References

1. D. Aggarwal, G. Brennen, T. Lee, M. Santha, M. Tomamichel, Quantum attacks on Bitcoin, and how to protect against them. Ledger **3** (2018)
2. G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, NISTIR8309: Status report of the second round of the NIST post-quantum cryptography standardization process, in *US Department of Commerce, NIST* (2020)
3. N. Anhao, Bitcoin Post-Quantum (2018). (Last accessed: 2022-Jan-15)
4. S. Bai, M.C.G. di Cirella, K. Karabina, T. Ngo, E. Persichetti, R. Steinwandt, PQC WIKI: A platform for NIST post-quantum cryptography standardization (Last accessed: 2022-Jan-15)
5. R.E. Bansarkhani, M. Geihs, J. Buchmann, PQChain: strategic design decisions for distributed ledger technologies against future threats. IEEE Secur. Priv. **16**(4), 57–65 (2018)
6. L.V. Bautista, M. León, F. Rodríguez, Performance analysis of e-cash protocols, in *Investigación para el Avance Educativo en Ciencias de la Computación*, pp. 24–28. Benemérita Universidad Autónoma de Puebla (2009)
7. D. Bernstein, T. Lange, eBATS (ECRYT Benchmarking of Asymmetric Systems). (Last accessed: 2022-Jan-27)
8. D.J. Bernstein, J. Buchmann, E. Dahmen, *Post Quantum Cryptography*, 1st edn. (Springer, Berlin, 2008)
9. W. Beullens, Improved Cryptanalysis of UOV and Rainbow, in *Proceedings of the Advances in Cryptology—EUROCRYPT 2021—40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Part I*, ed. by A. Canteaut, F. Standaert. Lecture Notes in Computer Science, vol. 12696 (Springer, Berlin 2021), pp. 348–373
10. D. Boneh, M. Drijvers, G. Neven, Compact multi-signatures for smaller blockchains, in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, Berlin, 2018), pp. 435–464
11. R. Campbell, Evaluation of post-quantum distributed ledger cryptography. The Journal of the British Blockchain Association **2**, 1–8 (2019)
12. A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, GeMSS: A Great Multivariate Short Signature (Last accessed: 2022-Jan-27)
13. Certicom, Standards for Efficient Cryptography Sec 2: Recommended elliptic curve domain parameters (2010)
14. K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, T. Schroeter, Blockchained post-quantum signatures, in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (IEEE, New York, 2018), pp. 1196–1203
15. D. Chaum, Blind Signatures for Untraceable Payments, in *Advances in Cryptology: Proceedings of CRYPTO '82, Santa Barbara, California, USA, August 23–25, 1982*, ed. by D. Chaum, R.L. Rivest, A.T. Sherman (Plenum Press, New York, 1982), pp. 199–203
16. V.B. Dang, F. Farahmand, M. Andrzejczak, K. Mohajerani, D.T. Nguyen, K. Gaj, Implementation and benchmarking of round 2 candidates in the NIST Post-Quantum Cryptography Standardization Process Using Hardware and Software/Hardware Co-design Approaches. Cryptology ePrint Archive, Report 2020/795 (2020). https://ia.cr/2020/795
17. J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, M. Kannwischer, J. Patarin, Rainbow Signature (Last accessed: 2022-Jan-27)
18. T.M. Fernández-Caramés, P. Fraga-Lamas, Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access **8**, 21091–21116 (2020)
19. I. Foundation, The Next Generation of Distributed Ledger Technology—IOTA (Last accessed: 2022-Jan-15)

20. P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU (2017)
21. Y. Gao, X. Chen, Y. Chen, Y. Sun, X. Niu, Y. Yang, A secure cryptocurrency scheme based on post-quantum blockchain. IEEE Access **6**, 27205–27213 (2018)
22. V. Gheorghiu, M. Mosca, A Resource Estimation Framework For Quantum Attacks Against Cryptographic Functions: Recent Developments (2021). (Last accessed: 2022-Jan-26)
23. C. Gidney, M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum **5**, 433 (2021)
24. D.O. Greconici, M.J. Kannwischer, D. Sprenkels, Compact Dilithium Implementations on Cortex-M3 and Cortex-M4, in *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021), pp. 1–24
25. L.K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, ed. by G.L. Miller (ACM, New York, 1996), pp. 212–219
26. S. Gueron, V. Krasnov, Fast prime field elliptic-curve cryptography with 256-bit primes. J. Cryptogr. Eng. **5**(2), 141–151 (2015)
27. J. Howe, PQCzoo: A platform for NIST post-quantum cryptography standardization (Last accessed: 2022-Jan-15)
28. A. Hulsing, D.J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M.M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, J.-P. Aumasson, B. Westerbaan, W. Beullens, SPHINCS+ a stateless hash-based signature (Last accessed: 2022-Jan-27)
29. M.J. Kannwischer, J. Rijneveld, P. Schwabe, D. Stebila, T. Wiggers, The PQClean project (Last accessed: 2022-Jan-15)
30. M.J. Kannwischer, J. Rijneveld, P. Schwabe, K. Stoffelen, PQM4: Post-quantum crypto library for the ARM Cortex-M4 (Last accessed: 2022-Jan-15)
31. C. Li, X. Chen, Y. Chen, Y. Hou, J. Li, A new lattice-based signature scheme in post-quantum Blockchain network. IEEE Access **7**, 2026–2033 (2019)
32. V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehle, S. Bai, Cryptographic Suite for Algebraic Lattices" (CRYSTALS) (Last accessed: 2022-Jan-27)
33. D. Moody, NIST Status Update on the Third Round (2021)
34. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2009)
35. NIST, Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (2016)
36. NIST, NISTIR8240: Status report of the first round of the NIST post-quantum cryptography standardization process (2019)
37. T. Okamoto, K. Ohta, Universal Electronic Cash, in *Advances in Cryptology—Proceedings of the CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11–15, 1991* ed. by J. Feigenbaum, vol. 576. Lecture Notes in Computer Science (Springer, Berlin, 1991), pp. 324–337
38. T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang, Falcon: Fast-Fourier Lattice-based Compact Signature over NTRU (Last accessed: 2022-Jan-27)
39. J. Proos, C. Zalka, Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Inf. Comput. **3**(4), 317–344 (2003)
40. QRL team, QRL: The Quantum Resistant Ledger (2016). (Last accessed: 2022-Jan-15)
41. M. Roetteler, M. Naehrig, K.M. Svore, K.E. Lauter, Quantum resource estimates for computing elliptic curve discrete logarithms, in *Advances in Cryptology—ASIACRYPT 2017, Proceedings, Part II*. Lecture Notes in Computer Science (Springer, New York, 2017), pp. 2.41–270
42. F. Shahid, I. Ahmad, M. Imran, M. Shoaib, Novel one time signatures (NOTS): a compact post-quantum digital signature scheme. IEEE Access **8**, 15895–15906 (2020)

43. L. Sharma, A. Mishra, Analysis of Crystals-Dilithium for BlockChain Security, in *Second International Conference on Secure Cyber Computing and Communications (ICSCCC), 2021* (IEEE, New York, 2021), pp. 160–165
44. R. Shen, H. Xiang, X. Zhang, B. Cai, T. Xiang, Application and implementation of multivariate public key cryptosystem in blockchain (short paper), in *Proceedings of the Collaborative Computing: Networking, Applications and Worksharing—15th EAI International Conference, CollaborateCom 2019, London, UK, August 19–22, 2019*, ed. by X. Wang, H. Gao, M. Iqbal, G. Min. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 292 (Springer, Berlin, 2019), pp. 419–428
45. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
46. W. van der Linde, Post-quantum blockchain using one-time signature chains. Master's thesis (Radboud University, Netherlands, 2018)
47. W. Yin, Q. Wen, W. Li, H. Zhang, Z. Jin, An Anti-Quantum Transaction Authentication Approach in Blockchain. IEEE Access **6**, 5393–5401 (2018)
48. G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, J. Katz, X. Wang, V. Kolesnikov, D. Kales, Picnic: A Family of Post-Quantum Secure Digital Signature Algorithms (Last accessed: 2022-Jan-27)

Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency

Michael W. Calafos and George Dimitoglou

1 Introduction

The conversion of illicit currency into legitimate assets to conceal unlawful activities is not new. The term "money laundering" was first introduced in the 1920s with the rise of organized crime syndicates in the United States (USA). The term originated from the use of local, predominantly cash-only laundromat businesses established with the sole purpose of concealing the proceeds from the activities of the notorious Al Capone. Under the direction of Capone's accountant, Meyer Lansky, several cash-type businesses, including casinos and nightclubs, were established to be used as cash fronts. Having a hard-to-trace cash business, it became possible to deposit the proceeds of illegal activities in banks, fund other businesses, and overall, avoid detection, seizure, and prosecution. By the time of his arrest in 1931 for tax evasion, Capone had laundered approximately $100 million (approximately $1.6 billion in 2021 money) and had created what would become the blueprint to conceal, convert, transfer, and legitimize illegally obtained funds [1–3].

Money laundering can range from simple courier-based cash transportation and conversion to portable high-value commodities to investments made using sophisticated financial transactions. Such transactions may involve financial institutions and, typically, cash-intensive legitimate businesses, including religious institutions and charitable organizations [1, 4, 5] along with purposefully established shell corporate entities and sham trusts. Although money laundering can conceal the proceeds of any criminal activity, it is a common predicate offense in drug distribution, white-collar crimes, bribery, corruption, and terrorism. The process can engage multiple knowing and oblivious individuals and organizations, ranging from

M. W. Calafos · G. Dimitoglou (✉)
Hood College, Frederick, MD, USA
e-mail: mwc4@hood.edu; dimitoglou@hood.edu

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_12

reputable financial firms and institutions, compromised or coerced employees and professional money laundering agents to shady money transfer companies, lawyers, accountants, insurance and real estate agents, commodity brokers, and dealers of high-valued goods and assets [1, 5].

The money laundering process can be a complicated, multi-stage activity, but it is generally identified by three distinct, sequential phases: *placement*, *layering*, and *integration* [1, 4, 6–12]. Placement introduces illicit funds into the financial system through simple cash deposits or more complex techniques. Layering creates layers of complicated financial transactions, such as opening multiple accounts in different financial institutions, transferring funds into offshore accounts with preference to institutions in jurisdictions with lax anti-money laundering laws and regulations [8–10]. Ultimately, the objective behind layering is to distance the illicit profits from their unlawful point of origin and obfuscate or, ideally, break the audit trail [1, 5, 7–12]. Placement and layering allow "dirty" money to be "washed," and be used in the integration stage [1, 5–12]. Integration uses the "cleaned" funds to purchase lawful assets and make legitimate investments via the purchase of legal, commercial enterprises and the acquisition of financial instruments that can produce capital gains and dividend income [1, 5, 6, 8–10]. Due to the inherently clandestine nature of money laundering transactions, it has been nearly impossible for authorities and law enforcement to reliably estimate the size and value of the international money laundering market.

Money laundering methods continue to evolve, the scope of operations expanding to a global scale, allowing technologically capable criminal enterprises to find new and "innovative" ways to exploit gaps in regulations and legal statutes. The sophistication of operations has also increased to include complex financial instruments, offshore accounts, credit cards, and wire transfers, along with engaging in diverse market and product areas such as real estate, charitable enterprises, antiquities, art, precious metals, aircraft, luxury goods, and natural resources [13].

The US Treasury's Financial Crimes Enforcement Network (FinCEN) attempted such a study in the late 1990s only to abandon the effort after 2 years due to too many unknown variables [14]. Similarly, between 1996 and 2000, the international Financial Action Task Force (FATF) on money laundering attempted a similar study, and it was also unsuccessful [1, 15, 16]. In 2011, the United Nations Office on Drugs and Crime (UNODC) estimated the annual global market value of laundered money between 1 and 5% of the global gross domestic product (GDP) [1, 10, 11, 15, 17, 18] with less than 1% of all illicit financial flows ever seized by authorities [19]. In 2018, the International Monetary Fund (IMF) estimated similar figures, with money laundering representing approximately 2–5% of global GDP or around $4 trillion [2, 5, 6, 15]. Some researchers suggest that these estimates may suffer from a ±20 percent estimation error, while others rank money laundering as the world's third largest industry behind oil and agriculture [2, 5].

The global acceptance of the Internet as a borderless, worldwide platform supporting business transactions, along with the development of virtual currency (cryptocurrency) [20, 21], has also contributed to changing the landscape of financial transactions and, subsequently, money laundering.

From an economic perspective, cryptocurrencies challenge how the value of a currency is determined and augment the strict classification of money as a commodity, credit, or fiat currency for storing value, functioning as a medium of exchange and serving as a unit of account [22]. Gold and silver are examples of commodity money with their value determined based on market supply and demand [23]. They have been used as mediums of exchange and, during the last century, as economic units backing physical fiat currencies. Credit money is non-interest-bearing receivables that cannot be redeemed on demand, a commonly recognized means of exchange with its value retained over the years. Fiat currency is a legal tender issued by a government or central banking authority in coins and paper. Its value is no longer backed by a gold or silver standard. The money itself has no intrinsic value, but its value is determined by a government or central banking decree, backing, and monetary policy [11, 22–24]. Unlike physical fiat currencies, a cryptocurrency's value is bound by the acceptance of individual market participants for that specific cryptocurrency [20, 21], supply and demand, and trust in the system [10, 11]. In addition, while fiat money can be printed continuously, potentially leading to high supply, resulting in inflation [23], cryptocurrencies have a fixed maximum supply limit, reached on a predetermined date, practically eliminating the risk of any inflationary pressure [11, 22, 25].

Technologically, cryptocurrencies are a decentralized electronic or digital means of exchange conducted over a borderless peer-to-peer (P2P) transaction network and anonymously recorded within a blockchain, a public, distributed transaction ledger [5, 10, 23, 24]. Cryptocurrency is a string of code generated by sophisticated encryption techniques and a complex cryptographic algorithm [10]. Cryptocurrency systems are decentralized and not controlled by an entity, government, or authority. Instead, transaction processing and validation are performed by a public community of cryptocurrency miners, who have agreed based on an a priori consensus mechanism on the particulars of the specific cryptocurrency process [21, 24, 26, 27]. The system provides anonymity as users are not required to disclose personally identifiable information (PII) to participate in financial transactions [8, 28].

This new economic and technology landscape has expanded money laundering capabilities by providing safe virtual environments to convert illegal, physical fiat currency into practically untraceable "cleansed" virtual assets. This type of laundering also follows the placement, layering, and integration phases, taking place on the Internet and the Dark Web [5, 9], at online auctions and gambling sites, on massively multiplayer online role-playing games, using unregulated financial intermediaries and exchanging value with various instruments, such as credit cards, prepaid cards, stored value cards ("smart cards"), mobile payments, and digital precious metals [9, 12, 13, 21, 28, 29]. Cyber laundering is effective, low cost, and hard to track and allows to engage in laundering transactions at a global scale quickly, efficiently, and anonymously [8, 10, 20]. It enables individuals and criminal organizations to launder large amounts of "dirty money" and operate at scale [7, 17] in multiple crime verticals. Traditional, physical criminal acts such as drug, weapon, and stolen goods smuggling, human trafficking, fraud, and extortion have been augmented with technologically savvy cyberspace crimes, such as cyberattacks, cyberwarfare, and cyberterrorism.

This chapter examines and compares traditional money laundering techniques with modern cyber laundering methods based on cryptocurrencies. We examine these methods and how they are used and discuss different practices, tools, and techniques. The work is structured to provide context and describe the evolution and transition of traditional money laundering into cyberspace and the related legal and regulatory challenges.

The remainder of the chapter is organized as follows. The following section provides an overview of money laundering, describing the different phases and the roles of participants. Section 3 introduces cyber laundering, including methods and tools. Section 4 compares traditional money laundering techniques with modern cyber laundering methods based on cryptocurrencies. In Sect. 5, there is an overview of both technical and nontechnical regimes and existing legal and regulatory frameworks to detect, investigate, and prosecute traditional and cyber laundering. Finally, the Conclusion section summarizes the topic and highlights technology and regulatory challenges as potential directions for future work.

2 Money Laundering

Possessing or spending higher amounts of money by individuals or organizations over what is expected to be obtained via legitimate means can trigger investigative and auditing actions by financial, regulatory, and law enforcement authorities. Money laundering transforms illegally obtained funds to various financial assets, concealing their source of origin and making it appear legitimate while introducing it into the financial system [14, 30]. The following sections describe the roles assumed by participants and the money laundering phases.

2.1 Roles and Participants

Money laundering begins with the *launderer*, playing the initial and coordinating role. Launderers can be classified under two broad types [3]: the *standard* vertical with three subcategories and the *professional* launderer.

The first type refers to either an individual acting alone or operating within a vertically integrated illicit organization engaged in the generation and subsequently laundering of illegal funds. Such launderers can be further classified into three organizational categories: *standard criminal*, *organized crime*, and *terrorist organizations*.

The second type refers to professional launderers that are one degree removed from the original activity which generated the illegal funds and they only participate in money laundering. They are considered a "weak link" because they can be easily deterred from participating as they are not career criminals but often have legitimate reputations, jobs, and careers or hold responsible roles in key institutions.

Traditionally, criminal organizations use money brokers or *controllers* recruited from within the organization's ranks for explicit purpose of trafficking and laundering money. However, as criminal enterprises become more sophisticated, it is common to recruit experts such as stockbrokers, money managers, commodity traders, lawyers, and accountants, to assist in their money laundering efforts. Their expertise increases the laundering effectiveness to benefit the criminal organization and, for the experts, the quick and substantial compensation if often enticing. Yet it comes at a high price of full responsibility, risk, and accountability if they get caught as it would be unlikely they would inform the authorities of who hired them and they would be subject to a wide range of possible punishment including fines, loss of professional licenses, and imprisonment.

In all cases, *launderers* often recruit and use couriers to distribute the money laundering tasks mostly to reduce the risk of or the impact of getting caught by the authorities with the entire amount to be laundered. Couriers typically convert large cash amounts to smaller amounts and make bank deposits in different accounts [8]. The roles of the launderers and the couriers vary within each of the different phases of the money laundering process.

2.2 Phases and Common Techniques

The motivation behind money laundering is to avoid detection of the predicate offenses by tracing the money trail, protecting the illicit proceeds from seizure, and using them without triggering suspicion of their origins [1, 5]. Therefore, the primary concerns for a money launderer are the speed, distance, and anonymity of each transaction [9]. A progressive three-step money laundering process transforms any "dirty" money into legitimate and usable "clean" assets (Fig. 1).

Money laundering begins with collecting and smuggling the proceeds ("dirty money") of domestic or international illicit activities. For example, for crimes committed in the USA, there is a strong incentive to smuggle and launder currency out of the country to protect it from detection and seizure enforced by bank-reporting laws.

It is, therefore, common to attempt smuggling funds into offshore banking havens in countries with either strong bank secrecy or lax bank-reporting laws. Once out of the USA, the funds can smuggle or repatriate back to the country using non-cash financial instruments, such as checks and debit cards. Over $50 billion is smuggled

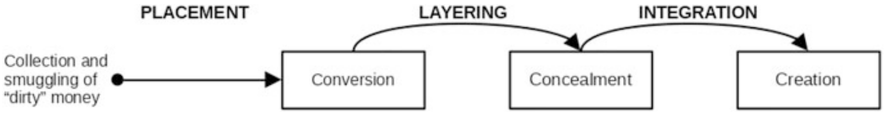


Fig. 1 The three phases (*placement*, *layering*, and *staging*) and their underlying objectives (*conversion*, *concealment*, and *creation*) during money laundering

out of the USA annually, with most funds crossing the US–Mexico border [31]. The smugglers use bulk shipping methods similar to transporting drugs, such as ships, containers, airplanes, and automobiles. Other ways to smuggle cash are individual couriers or currency mules or postal mail to change cash into negotiable instruments, such as traveler's checks and money orders.

2.2.1 Placement

Placement is the first phase in the money laundering process and involves converting illicit funds into smaller, more manageable, transportable, and less suspicious amounts by directly placing the proceeds into the mainstream financial system [1, 4, 6–11, 18, 31, 32]. This conversion makes the illicit funds more liquid and appears legitimate. While placement can be accomplished in various ways, the launderer's sophistication, access to resources, and geographical location play a significant role in selecting the most suitable methods. In general, after breaking down the funds into smaller amounts, numerous couriers, also known as *smurfs*, under the direction of a money launderer deposit the amounts into several financial accounts at different locations on various days. This method aims to avoid triggering any anti-money laundering (AML) reporting requirements and is referred to as *structuring* or *smurfing* [8]. Alternatively, exchanging funds for traveler's checks, money orders, or debit cards [6, 8] is less likely to trigger detection. Similarly, channeling funds through casinos is also common as long as they are in jurisdictions—unlike casinos under US jurisdiction—that have no reporting requirements when converting cash to chips and vice versa [33].

Funds can also be channeled through "front" operations, such as restaurants, nightclubs, or via informal, shadow, and nontraditional financial systems, such as unregistered exchanges or hawalas [5, 6, 8]. A hawala is a trust-based alternate payment system in Southeast Asian countries, which involves an agent known as a hawaladar and does not leave a money trail. An individual wanting to transmit funds to another country deposits money with a hawaladar. For a fee, the hawaladar arranges with a hawaladar in the destination country for the funds to become available. A code is used between the parties to receive the funds, and the two hawaladars reconcile the accounts using regular trading practices or couriering precious metals or gems across borders [5, 34].

2.2.2 Layering

Layering is the next step in the money laundering process to create complicated financial transaction layers. Practically, multiple complex transactions are initiated through various institutions and jurisdictions. The main objective is to further distance illicit profits from their unlawful and suspicious point of origin and break the audit trail [1, 5, 7–12, 18, 31, 32]. Frequently shifting funds throughout the financial markets obfuscates the money trail and generates confusion, so the funds become untraceable, making each transaction viewed in isolation resemble legal, financial activity [5, 31].

Another factor to any *layering* operation's success is to ensure that transactions, whether performed physically or electronically, cross through multiple national borders and corporate structures. As more layers are introduced, the more complex the scheme becomes and the more difficult it becomes for authorities to trace and investigate. Similar to the *placement* stage, *layering* includes opening numerous physical or online accounts at different financial institutions [9] and transferring funds into offshore accounts [8, 31]. The target financial institutions are carefully selected under weak financial monitoring or banking secrecy laws. The most straightforward yet effective *layering* technique is to electronically wire transfer funds to such offshore banking heaven jurisdictions before rerouting the funds to another location or business entity. An alternative to using financial institutions is *layering* by establishing multiple cross-border shell companies, such as import-export businesses, travel agencies, and money-service businesses, and routing funds to these companies [6, 31].

Overall, the more methods, financial instruments, and shell companies engaged in the process, the more complex and challenging the laundering trace becomes. Some of the standard techniques to transfer and justify funds are wire transfers, bank drafts, false invoices, over-invoicing, dollar discounting through money orders, or counterbalancing loan structures [31]. Counterbalancing loan schemes, in particular, tend to launder more significant amounts as they involve depositing illicit funds into an offshore account and then using the account as collateral to obtain a bank loan in another country. Finally, *layering* may also include converting cash deposits into other forms of financial instruments, such as checks, commodities, futures, bonds, stocks, and cryptocurrencies [6, 8–10].

2.2.3 Integration

The third and final step in the money laundering process is *integration*. In this step, the "washed" money is reintroduced and integrated into the legitimate financial system and economy [1, 5–12, 18, 31, 32]. Once this conversion occurs, the "washed" money is considered fully laundered [8, 10]. Its illicit origins are untraceable, and the funds can be used to purchase lawful assets and make legitimate investments while creating an appearance of legitimacy [5, 6, 8]. These acquired assets and investments may include equipment to support future criminal pursuits, income-generating commercial enterprises, such as real estate and cash-intensive businesses, or profits from financial instruments that can produce capital gains or dividend income [1, 6, 8, 10, 18, 31].

This last step is often the more visible and most dangerous for the launderers as the "owners" of the laundered funds become active, open participants in the legitimate market. It is often at this stage that extravagant, out-of-the-ordinary purchases or investments by those suspected of criminal activity get the attention of the authorities and can trigger investigations to determine the origins of the funds.

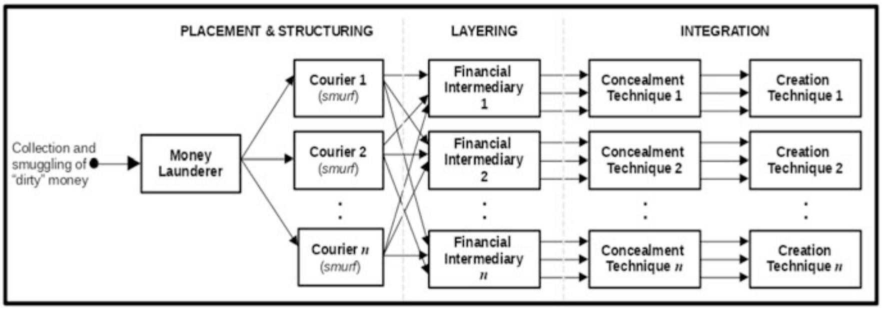


Fig. 2 The full flow of traditional money laundering activities, including at each stage, multiple couriers, financial intermediaries, and techniques

Integration failures on the part of money launderers can cause prosecution along with asset and account seizures by authorities and may lead to additional findings related to predicate criminal organization activities.

After this phase, the original funds are practically entirely diluted. While the money laundering process looks linear (Fig. 2), the number and variety of transactions, currencies, assets, and financial instruments make it too complex to be detected, let alone to successfully trace back the origins of the laundered funds or the predicate crime.

3 Cyber Laundering

The widespread use and availability of online services offer criminal organizations new ways to improve their money laundering operations. Cryptocurrencies have provided an additional way to avoid detection, maintain anonymity, and have a global reach, moving traditional money laundering into the realm of cyber laundering [8–10, 20, 27]. Cyber laundering may be conducted partially or fully online, with the cross-border and cross-jurisdiction transfer and laundering of cryptocurrencies performed covertly, seamlessly, and practically instantaneously [8–10, 23]. As it is relatively straightforward to establish an online identity using a digital front or shell company in many parts of the world [8, 12], moving funds domestically and internationally becomes effortless. Multiple online accounts or shell companies can be established during *layering* to spread funds across locations and jurisdictions before integrating them into legitimate financial systems. These online accounts and shell companies can also be used to integrate fiat currency into the financial system by making the shell company's accounts, income, payments, profits, services, and products seem legitimate [9].

A simple way to obfuscate and make cryptocurrency transfer into the financial system look less suspicious is through the practice of *micro laundering*, breaking up significant cryptocurrency amounts into smaller amounts, then exchanging them for fiat currency, and depositing them into legitimate accounts [35]. Combining *micro laundering* with readily available cryptocurrency mixing/tumbler services and privacy-preserving tools [5, 13, 20, 21, 28, 29, 36], launderers are able to further anonymize transactions, preserve privacy, and avoid detection by the authorities.

Interestingly, unlike fiat currency, cryptocurrency can be used both as an input and as an output asset and can enter or exit the laundering process at any stage. Cryptocurrency holders can use unregistered exchanges or other financial intermediaries, bypassing the established financial and banking system, along with any other regulatory authorities, and any *know your customer* (KYC) verification requirements [8, 12]. Similarly, cyber launderers use unregistered exchanges to convert fiat currency and even precious metals and gems into cryptocurrencies avoiding regulatory scrutiny.

While these methods bypass detection, the underlying online and network infrastructures generate copious amounts of Internet-based transaction activity logs. Even an ordinary website visit automatically generates activity log entries on the user's computer, the Internet service provider's (ISP) network, and the website server. The entries vary in detail, but at minimum, they include Internet Protocol (IP) address information and the protocol types used. To address this, launderers deploy a number of methods as logged activities present an unwanted trail of electronic evidence.

3.1 Cyber Laundering Methods

Launderers use an arsenal of tools and techniques to hide their transactions and thwart the generation of dependable and traceable logs that could be used by law enforcement and regulatory agencies. Software like The Onion Router (TOR) is an example of an easily accessible, free, anonymization application that uses multiple TOR nodes to route traffic through the Internet while encrypting traffic between the nodes. Since the IP address of only the previous node is detectable to a connecting computer, the software conceals the originating IP address and the subsequent trail [13, 28, 37].

Besides the use of anonymization software, other standard methods include the use of mixing/tumbler services, encryption, proxy servers, virtual private networks (VPNs), IP spoofing techniques, unauthenticated Wi-Fi "hot spots," and prepaid phones as modems to connect to the Internet [9, 38, 38]. A unique and very effective approach is using mixing/tumbler services.

3.1.1 Mixing/Tumbling Services

Mixing/tumbling services mix legitimate with illicit cryptocurrency, converting "dirty" into "clean" cryptocurrency and concealing the transaction history on the blockchain. The "clean" cryptocurrency is obtained from other legitimate users of the service. Therefore, the higher numbers of legitimate subscribers increase the efficacy of the mixing/tumbling. The mixer gives cleansed cryptocurrencies a new public address from one of the mixer's "clean" public addresses unrelated to the mixing/tumbling process. The mixing service deducts its transaction fee from the clients newly "cleansed" funds and refills its cryptocurrency reserves from cryptocurrencies in public addresses, contributing to the mixing process.

For returning customers, including serial launderers, the mixing service issues the customer a returning customer number after each mix. Tracking the customers prevents the mixing service from paying out the customer with tainted cryptocurrency deposited in its reserve when the same customer reuses the mixing service. Users of the mixing service can check the taint of their received cryptocurrency at the blockchain, but if the mixing/tumbling is executed correctly, there should be no linkage or *zero percent taint* [13, 37]. In addition, mixing service providers often clean their cryptocurrency through their service and then convert it into fiat currency, benefiting from their proceeds without revealing their identity or ownership status.

Practically, once illicit cryptocurrency has been mixed/tumbled and commingled with legitimate cryptocurrency, it becomes disassociated from its transaction history.

Legitimate mixing services can be licensed and regulated by financial authorities for businesses to exchange different virtual currencies [37]. However, while it might be technically complex, it is easy to set up such a service and operate without registration and license. While both the operators and those using unlicensed mixing services are subject to severe penalties that include fines, imprisonment, and confiscation of assets [37, 39], their detection and prosecution are challenging as most such services also use anonymization tools to conceal their activities.

3.1.2 Cards

Credit and prepaid cards, also known as "smart" cards, are stored value instruments. Due to their prevalence in use for e-commerce, the use of stolen or forged cards to buy products and services purchased online is very common [40, 41]. Although cyber launderers can use credit cards, the preferred payment method is using prepaid cards. Prepaid cards use either an open or a closed system.

An example of *open system cards* is debit cards, which are backed by fiat currency and can be used almost anywhere, including conventional automated teller machines (ATMs), convertible virtual currency (CVC) kiosks, or crypto ATMs. These crypto ATMs allow exchanging fiat currency or e-money for cryptocurrency [9, 39].

On the other hand, an example of *closed system cards* is prepaid telephone cards which can be bought and resold. No matter the system used, prepaid cards can be used during every money laundering stage, and they are highly valued for their ease of use in transferring funds across borders.

3.1.3 Online Auctions

Online auctions are commonly used to place and layer illicit proceeds into the bank accounts of legitimate, typically shell companies. A shell company representative serves as the item in the auction, and *smurfs* act as buyers, driving the item's price for sale as high as possible. As auctions do not have price limits, the *smurfs* make bids of exorbitant amounts compared to the value of the auctioned item. Then the *smurf* with the highest winning bid sends the "dirty" money to the seller's bank account. Next, the seller ships the item once the funds have cleared the bank, completing the transaction. Since a reputable, albeit a shell, company is involved in the process, it gives the transaction the appearance of legitimacy [9].

3.1.4 Online Services

Online services refer to services provided by online banks and other virtual financial intermediaries, such as PayPal. These are attractive laundering instruments as it is easy to exploit regulatory differences and bypass requirements, such as opening Internet bank accounts in different jurisdictions. Accounts may be opened under the name of a shell company providing fake or real services and products to conceal identity and give an additional appearance of legitimacy. By providing real services or products, legitimate customers unknowingly provide lawful proceeds which are blended with unlawful proceeds, making the distinction and tracking of the latter, harder to detect. It is not uncommon for online services to cover unregistered peer-to-peer (P2P) cryptocurrency exchanges where cryptocurrencies or fiat currency can be exchanged. These exchanges frequently use mixing/tumbler techniques and even money couriers, known as *money mules*, to infuse more anonymity and transaction concealment. Transactions between a client and an exchange are possible using crypto ATMs, although a crypto ATM can also be used directly as an exchange by itself [39].

3.1.5 Online Gambling

As with real-world gambling, online gambling is another quick and efficient way of legitimizing illicit funds and tax evasion. Typically, offshore casinos in locations with lax regulations are chosen, and they can be used to launder and distribute large amounts of money. A typical method is by exploiting legal Internet-based gambling services or setting up illegal gambling businesses. Either way, online gambling is an effective cyber laundering method since most transactions use credit or prepaid cards [9, 42].

3.1.6 Virtual Money Laundering

Virtual money laundering is a comparatively new technique using Internet-based charities and massive multiplayer online role-playing games (MMORPG). Cyber launderers donate dirty money to seemingly legitimate shell companies, established as Internet-based charities doing minimal or no charitable work. With MMORPGs, on the other hand, a money laundering player can virtually purchase cryptocurrencies using fiat currency at a fixed exchange rate before playing and then earn more cryptocurrency while playing the game. The player can then virtually exchange the cryptocurrency with others or buy or sell virtual items. The player can also convert the cryptocurrency for fiat currency and then deposit the fiat currency into one or multiple accounts. Once the fiat currency is deposited, the player can withdraw it from any ATM. Occasionally, players get reloadable debit cards to play a particular game, which also allows a player to withdraw fiat currency from ATMs [9].

3.1.7 Mobile Payment Services

Mobile payment services (MPSs) are offered by non-banks and do not require a user to have a bank or credit card account. Mobile payments, also known as m-payments [14], are transacted over a mobile phone or other communications device, connecting to the Internet through voice access, text messaging, or wireless application protocols to make payments [9]. MPSs can operate under two business models [9, 41].

In the first business model, a telecommunication operator is the financial intermediary to authorize, clear, and settle payments between the mobile service provider and the uses. Doing so allows users to use their mobile phones at a merchant's point of sale (POS).

In the second business model, a cryptocurrency, as an electronic currency, can be stored on a mobile phone or a mobile phone account. It can then be transferred to other users or converted into or from fiat currency [41]. Prepaid mobile phones can also be used for mobile payments like prepaid cards and provide an extra layer of anonymity as single in-line memory module (SIMM) cards used in prepaid mobile phones do not require registration or reveal of the buyer's identity [9]. Mobile phone payments have replaced bank accounts in numerous countries and payments through banking instruments (e.g., cash, checks, money transfers). Especially in countries with underdeveloped or poorly functioning banking systems, MPSs are the fastest way to conduct business [41]. Cyber launderers use mobile phones for the *layering* and *staging* phases, also known as *digital smurfing* [14]. They direct multiple *runners* with mobile phones and illicit fiat currency to m-payment establishments to exchange the fiat currency for electronic currency. *Runners* first download the electronic currency to their mobile phones. Then, they follow specific instructions by the launderer to forward the credited electronic currency to master accounts or to transfer the funds to some other directed location.

3.1.8 Digital Precious Metals

Using digital precious metals (DPMs) allows cyber launderers to perform online transactions without using foreign exchanges or worrying about the underlying currency. DPMs rely on exchanging derivatives options, giving a cyber launderer the right to purchase an amount of virtual precious metal holdings at a specific price based on the current price of the precious metal on the global commodity exchanges. Since a DPM is an option, it can be exchanged like any other traditional commodity or derivative security. Once the cyber launderer has obtained an amount of DPMs, they in whole or in part can be transferred to other individuals or exchanged for goods and services. Performing these transactions over the Internet makes it difficult for a DPM dealer to verify a customer's real identity [9].

3.1.9 Ransomware Campaigns

A ransomware campaign against select targets is another standard method of cyber laundering. This type of hacking attack is based on ransomware, a type of malicious software or malware that infects a computer system to obtain or remove data and hold the data hostage. Once the system is compromised, the ransomware blocks access to the data. The attacker then contacts the target and demands a ransom payment to release the data, usually in the form of a cryptocurrency. It is also common for the attacker to threaten the target to release or publish the data for non-payment. The attacker can be an individual hacker or a hacker group working alone or with a criminal organization or even a rogue state. It is not uncommon for criminal organizations to purchase the necessary ransomware and hacking tools, hire hacking talent, hardware, software, and even already compromised personally identifiable information (PII) with illicit funds before the attack [21, 22, 36]. Upon payment of the ransom from the target, they hold "clean" cryptocurrency.

4 Traditional vs. Cyber Money Laundering

Traditional, physical, in-person laundering practices have evolved, moved, or expanded partially or fully in cyberspace. The multitude and complexity of online tools make cyber laundering seem entirely different from the operational methods of its pre-Internet predecessor, although it is interesting to compare and analyze the differences.

The analysis assumes that any financial intermediaries can be operating in any type of jurisdiction, neutralizing for the sake of the comparison the impact of strict, strong privacy, lax, or non-existent anti-money laundering regimes. Although not always feasible, it is clear from the perspective of the launderers that non-strict or strong privacy regimes are the preferred localities to execute money laundering transactions.

This comparison intends to identify similarities and differences from both the launderers' and authorities' perspectives. The structure of the comparison is framed on the three phases of money laundering (*placement*, *layering*, and *integration*) since these phases seem to be common.

4.1 Placement

In the traditional, physical money laundering environment (Fig. 2), the money launderer uses numerous couriers to fulfill the initial structuring of the "dirty" money within the *placement* stage by physically giving each courier bulk amounts of "dirty" money. Each courier breaks up their amount into multiple smaller amounts[1] and then deposits (places) them into various regulated (e.g., banks, currency exchanges) and unregulated financial intermediaries (e.g., hawalas, shadow banks, unregistered exchanges) for the "dirty" money to be converted and appears as "clean" money deposits. With cyber laundering, the launderer does not rely on couriers to fulfill the initial structuring within the *placement* stage (Fig. 3). Instead, the launderer purchases cryptocurrency directly over the Internet (e.g., in the Dark Web) or through illicit cryptocurrency exchanges. The "dirty" cryptocurrency is then virtually converted ("cleansed") using special mixing/tumbler software or unregistered mixing/tumbler service providers. Various amounts of the "clean" cryptocurrency are deposited (placed) into multiple cryptocurrency blockchains and virtual wallets, avoiding regulated financial intermediaries and reporting requirements.

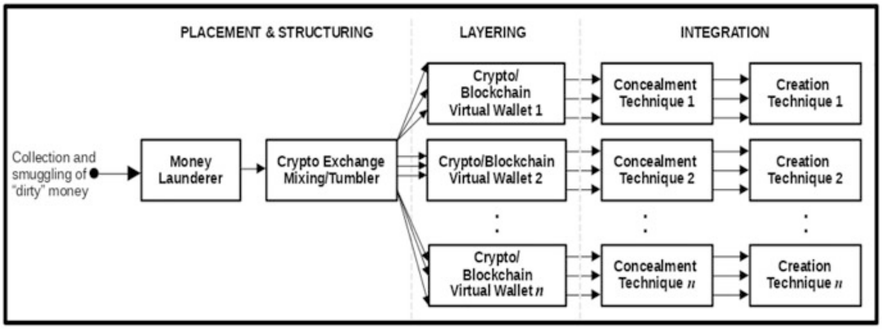


Fig. 3 The full flow of cyber laundering activities at each stage of money laundering. Leveraging cryptocurrency exchanges and virtual wallets, The Placement & Structuring and Layering phases are simplified and can be carried out even by a single person

[1] In the USA, this amount is under the $10,000 reporting requirement threshold.

4.2 Layering

Layering aims to further distance already structured, “cleaned” funds from their illicit origin to hinder detection. With traditional money laundering, the launderer attempts to use the funds for legal purchases, electronically transfer funds to other locations, and make investments using legal financial instruments. Purchases and transfers are carried out using legitimate wire transfer services, currency exchanges, smart cards, and mobile payments (m-payments). Investments are made in stocks, bonds, commodities, derivative securities (forward, futures contracts, options, and swaps), other fiat currencies, and cryptocurrency.

Similarly, cyber laundering attempts to use structured funds for *layering*, although there are operational differences. The money launderer can either directly use “clean” cryptocurrency from a blockchain or virtual wallet or convert the “clean” cryptocurrency to “clean” fiat currency for purchases, transfers, and investments. This is a significantly simpler and less labor-intensive aspect of this phase compared to traditional laundering.

4.3 Integration

After the additional concealment and complexity *layering* stage, the further cleansed funds are available for use and incorporation into the legitimate financial market. The modus operandi for using the cleansed funds at the *integration* stage matches the available methods and options during the layering stage. Again, the funds are used to purchase assets and make legitimate investments using legal, financial instruments. Although *integration* provides another layer of concealment, the sole intention is not to hide the money but to engage in for-profit activities or support future criminal actions. Typically, purchased assets favor real estate and luxury items, such as art, antiquities, jewelry, automobiles, watercraft, and aircraft. At the same time, investments besides typical financial instruments may also include cash-intensive business ventures.

Overall, the process does not seem dramatically different than traditional money laundering (Fig. 3). However, it is clear that the use of cryptocurrency offers cyber launderers significant operational advantages in terms of profit, speed, and reducing the risk of detection (Table 1). The use of cryptocurrency has at least two inherent factors that make it more effective in every stage of the money laundering process (Table 2). First, it is the *quasi-anonymity* afforded by cryptocurrencies, which plays a significant role in minimizing the ability to track and follow the money trail both during and after the transactions are complete. Second, the high-speed, *real-time transactions* make detection difficult during the fund transfers, while jurisdictional conflicts make regulatory enforcement and prosecution difficult.

From a process perspective, the use of exchanges at the *placement* phase and subsequently the use of cryptocurrency and virtual wallets at the *layering* phase have

Table 1 Comparing traditional money laundering with cyber laundering activities at each stage of the process

Comparison of Traditional Money Laundering vs. Cyber Laundering			
	Placement	Layering	Integration
Traditional activity	***Structuring*** • Multiple couriers ("smurfs"). ***Conversion*** • Multiple financial intermediaries.	***Concealment*** • Use fiat currency to buy/sell financial instruments, fiat and crypto currency. • Wire transfer fiat currency.	***Creation*** • Use fiat currency and crypto currency to buy legitimate assets, make investments.
Cyber activity	***Structuring*** • Unregistered exchange. • Mixing/tumbler service or software. ***Conversion*** • Multiple blockchains, virtual wallets ("digital smurfing").	***Concealment*** • Use crypto currency to buy/sell financial instruments, fiat and crypto currency. • Wire transfer of crypto currency.	***Creation*** • Use crypto currency to buy legitimate assets, make investments.

Table 2 During the money laundering process, the use of cryptocurrency offers certain advantages over fiat currency based on two general factors: *quasi-anonymity* and *real-time transactions*

Advantages of Cryptocurrency During Money laundering Stages			
General factors	Placement	Layering	Integration
Quasi-anonymity	Used by Illicit organizations and their associates	Difficulty in matching names with transactions	Anonymous and untraceable cashing out of proceeds
Real-time transactions	Cross-border transference to another cryptocurrency	Limited lead time to stop suspicious transactions	Quick cross-border movement and withdrawal of illicit proceeds

the most significant impact. Compared to the same traditional money laundering phases, laundering activities can be carried out by a single actor, who is able to mix funds and then distribute them to virtual wallets without having to engage multiple couriers or interact with financial intermediaries.

The effectiveness of cyber laundering techniques creates significant challenges in the detection, investigation, and prosecution of launderers.

5 Investigating, Regulating, and Prosecuting Cyber Laundering

Cyber laundering investigations are complex and time-consuming that typically only the largest investigative agencies with the most skilled and technical savvy personnel have the resources to pursue with any degree of success. Investigators must thoroughly understand cryptocurrency and blockchain technologies and the complex transaction methods and algorithms they support. They must also keep pace with an accelerated rate of innovation within the cryptocurrency market that constantly introduces different currencies with varying anonymity and payment systems [5, 6, 10, 22].

The heavy use of encryption to support anonymity and its application with digital wallets notably increases the challenge for investigators to identify those involved in transactions [21, 43, 44]. While a user's public keys may be traceable through transaction histories, the existence of potentially numerous public keys associated with an individual makes the investigative tasks only more complicated. Even when identifying information, such as PII, is required to confirm a user's identity and open an account, the users can still provide fraudulent information [20]. The users can also conceal their identities using multiple public addresses from different cryptocurrency wallets or connecting to other computers within an open wireless network [37]. The latter technique is particularly concerning since unsuspecting, unaware, innocent individuals can be hijacked and become part or inadvertently support illicit communications and activities.

Overall, these investigative challenges are inherent in the cryptocurrency and blockchain environment. As the popularity of blockchain usage increases and sophisticated analytical techniques, strategies, and tools are developed, novel investigation techniques into blockchain transactions may become more accessible for the anti-money laundering, regulatory, and enforcement communities [37]. At this time, this is not the case, positioning law enforcement and regulatory authorities at a significant disadvantage.

Two other challenges to investigation and enforcement are the lack of clear regulations about cryptocurrency and standard international enforcement or a uniform legal framework relating to cyber laundering. The opinions and rulings of legal authorities vary on the definition and classification of cryptocurrencies, making enforcement and especially prosecution difficult [17, 21, 26]. Unlike traditional money laundering, some standardized anti-money laundering frameworks tend to exist [1]. While they typically rely on a flexible risk-based approach instead of a rigid rule-based approach to counter money laundering [10], this is not the case with cyber laundering. This lack of a standardized, anti-cyber laundering framework hinders the cooperation, investigation, and prosecution efforts between law enforcement authorities and lawful stakeholders, especially in cases involving cross-border, cross-jurisdiction activities [5].

5.1 Money Laundering Legislation and Regulations

The lack of a comprehensive, international regulatory framework imposes several challenges to law enforcement. In this section, we focus on the US anti-money laundering (AML) regime, which seems to be one of the earliest and more mature regimes.

The first instance of AML legislation in the USA originated in the 1970s. Although tax evasion and dealing in stolen goods are closely linked with money laundering and were always considered illegal, it was not until the US Bank Secrecy Act (BSA) was passed as a component of the war on drugs [1, 6, 11, 26, 37] that made money laundering per se to be considered unlawful. In the USA, the Department of the Treasury's Office of Terrorism and Financial Intelligence (TFI) is charged with combating money laundering. At the same time, the Financial Crimes Enforcement Network (FinCEN) bureau, established in 1990, has an active role in gathering financial intelligence, enforcing regulations, providing guidance on compliance issues, and assisting other agencies to prevent money laundering and other financial crimes domestically and internationally [6, 11, 37, 45].

Existing federal anti-money laundering laws criminalize money laundering and other associated acts. The foundation for such laws was the passing of the BSA and later, the Money Laundering Control Act (MLCA) of 1986 [1, 6, 7, 17]. The passing of these Acts influenced the creation of similar legislation in other countries as most countries lacked regulations addressing AML controls. It also helped guide the formation during the 1989 G-7 Summit in Paris of the Financial Action Task Force (FATF), an international AML policy-making association of member nations charged with developing international AML standards [1, 6, 46].

Later, the scope of these two Acts, along with the Treasury Department's enforcement powers, was greatly expanded with the passage of the USA PATRIOT ACT (Patriot Act) after the September 11, 2001, terrorist attacks [1, 6, 7, 11, 37].[2]

These laws depend on the reporting, record-keeping, and enforcement of various financial and certain non-financial institutions [1, 17]. Two such standards that institutions must follow are the completion and transmittal to the US Department of the Treasury of Currency Transaction Reports (CTRs) for any domestic over $10,000 or any international over $5000 cash transaction and Suspicious Activity Reports (SARs) for suspicious transactions [1, 6, 7, 11, 17, 26, 37]. Additionally, institutions must have and maintain an anti-money laundering compliance program.

The above legal and regulatory elements compose the US anti-money laundering (AML) regime based on prevention and enforcement (Table 3). The prevention

[2] There is a standing disagreement between legal scholars on the coverage of section 359(a) of the Patriot Act. Some argue that it extends the MLCA's reach to include the Internet and emerging technologies, therefore equating cyber laundering to traditional money laundering in terms of civil and criminal sanctions. Others argue that the section does not specify Internet-based technologies but amends the BSA definition of a "money transmitter" so that informal or underground banking systems are treated as financial institutions subject to BSA regulations and sanctions.

Table 3 The US anti-money laundering (AML) regime is based on, *prevention* and *enforcement*, each with its key activities and respective actions

Regulatory agencies		Criminal investigative agencies	
Prevention		Enforcement	
Activities	Action(s)	Activities	Action(s)
Sanctions	• Administrative/regulatory • Civil/criminal penalties	**Confiscation or Forfeiture**	• Asset seizure
Regulation & Supervision	• External compliance audits	**Prosecution and Punishment**	• Civil/criminal penalties
Reporting	• Reports/info to authorities	**Investigation**	• Based on reports, info to authorities
Customer Due Diligence (CDD)	• Account holder’s name • Proof of identity. • Ongoing account monitoring	**Underlying Offenses or Predicate Crimes**	• List of predicate crimes. • Legal basis for money laundering criminalization. • Only funds associated with predicate crimes subject to AML laws.

aspect is designed to discourage illicit actors from using lawful institutions to launder “dirty” money and legitimate institutions from collaborating with illicit actors by requiring transparency in transactions. The enforcement aspect acts as a punishment mechanism against illicit actors and their accomplices [1, 11].

From the perspective of cyber launderers, these legislative actions present potentially increased risks of fines, seizure of assets, arrest, and prosecution. To mitigate these risks, they can often devise costly schemes to bypass regulatory controls and avoid detection, which becomes a challenge of balancing economic incentives. So for them, one option is to continue with “business as usual’ as the current risks are low. A second option is to attempt to devise and engage in complex laundering methods at a very high cost to reduce risk as much as possible. A third option is to use a different, less risky money laundering techniques that may be slower to carry out or much harder for them to access the laundered proceeds. Finally, the fourth option, which meets the deterrence aspect of controls set by the authorities, is to abstain from money laundering altogether by recognizing that the economic benefit may not be worth the cost and risk of detection and inevitably prosecution [11].

Unfortunately, at this time, the first option seems to be dominant choice as cyber laundering offers scale, low operational costs, and realistically, it is low risk given that is easy to evade the few anti-money laundering controls currently in place or the understaffed and under-resourced authorities.

5.2 *Cyber Laundering Legislation and Regulations*

Most regulatory schemes and legislative policies regarding cryptocurrency and cyber laundering, particularly at the international level, are fragmented and do not adequately address the cryptocurrency market [17, 21]. This fragmentation ranges from some jurisdictions altogether banning the use of cryptocurrency due to its perceived threat to other jurisdictions not having any laws because they do not consider cryptocurrency as currency and therefore not subject to anti-money laundering regulations. Even cryptocurrency's monetary and legal definition varies between jurisdictions and sometimes even among agencies within the same jurisdiction [13]. These variations in defining, recognizing, and regulating cryptocurrency within a legal context allow illicit cryptocurrency activities to thrive and impede the effective international regulation and enforcement of cyber laundering [5, 21].

The USA has been more deliberate in regulating cryptocurrencies and enforcing violations than many other countries, but even within the USA, policies concerning cryptocurrency vary on an individual state level [6, 11, 45, 46]. The US Treasury Department's Financial Crimes Enforcement Network (FinCEN) bureau is one of the few agencies within the federal government that has an active role in issuing guidance relating to cryptocurrency and has most likely enough authority to regulate cryptocurrency. FinCEN is charged with gathering financial intelligence, enforcing regulations, providing guidance on compliance issues, and assisting other agencies domestically and internationally in its anti-money laundering mandate. Based on the bureau's analysis of cryptocurrencies and the US Bank Secrecy Act (BSA) of 1970, in 2013, the bureau determined that the act also applies to cryptocurrencies [6, 11, 23, 37, 45, 46]. According to FinCEN guidelines, entities operating within the cryptocurrency market can fall into three categories: users, exchanges, and administrators.

- *Users* are individuals that mine (create) or use cryptocurrency to buy real or virtual goods or services. Because these individuals are not normally engaged in a money transmission service, even if they created the cryptocurrency, the federal statute regarding money service businesses (MSBs) does not apply in most situations [11, 37, 47]. Conversely, the users may become exchangers under BSA and subject to MSB regulations if they act as an intermediary accepting and transmitting cryptocurrency between two parties. Additionally, the users may become money transmitters if they sell cryptocurrency to buy fiat currency, equivalent, or another cryptocurrency.
- *Exchanges* are firms that are in the business of accepting, buying, and selling cryptocurrencies to exchange such funds for fiat currency, other funds, other cryptocurrencies, and, therefore, providing money transmission services. These firms meet the definition of a money exchanger under BSA; they are subject to MSB regulations, including registration, reporting, and record-keeping requirements [6, 11, 37, 48]. The vast majority of states require any firm transmitting funds between two parties to acquire an operating license. This license is required for consumer protection and to reduce default risk since most money transmission

businesses are not insured by the Federal Deposit Insurance Corporation (FDIC), as are commercial and savings banks.

- *Administrators* refer to individuals in the business of placing into circulation or issuing cryptocurrency and by authority can withdraw from circulation or redeem cryptocurrency [11, 48]. The cryptocurrencies, in this case, are generally centralized ones [11], such as Ripple. Since administrators are transmitting cryptocurrency, they are also included under the BSA definition of a money exchanger or transmitter and subject to MSB regulations.

While these categories provide a systematic classification of the actors in the cryptocurrency space, they are not comprehensive. There is often confusion when attempting to enforce relevant guidelines as statutes are unclear to the definition of "acting as a business," leaving the definition open to interpretation. In the situation of miners, for example, they can sell or trade a large portion of a Bitcoin portfolio for a good or service and not be subject to MSB regulations, but if they sell a fraction of bitcoins to a friend from their portfolio, they may be subject to MSB regulations [11].

While the overarching legislative and enforcement frameworks evolve and mature, specific nontechnical and technical controls can interfere with and disrupt or discourage cyber laundering activities.

5.3 Nontechnical Regimes Against Cyber Laundering

There are several principles and practices that implement controls toward strengthening money laundering prevention efforts.

5.3.1 Know Your Customer and Customer Due Diligence

A set of fundamental concepts within any anti-money laundering regime are the principles of Know Your Customer (KYC), and Customer Due Diligence (CDD) [7, 10, 21, 38]. KYC and CDD controls are in place to prevent both money laundering and terrorist financing. Their controls are mandated by law for firms within the financial service industry, requiring firms to substantiate any person holding or listed on an account. These controls appear at various phases of the customer relationship, with each phase requiring a different control [10]. Once identities have been confirmed and established, constant risk assessments and monitoring of accounts are required. If any transaction meets the requirements for issuance of a CTR or SAR, notification and the report are forwarded to the appropriate authorities for possible investigation [37, 38]. The more effective an anti-money laundering control is, the more challenging and riskier it is for illicit actors to successfully launder their money [21].

When considering cryptocurrency exchanges, KYC/CDD can be a useful cyber laundering detection tool, particularly within jurisdictions with strict regulations. Additionally, the mandatory use of CTRs and SARs is a serious first step in removing anonymity from cryptocurrency networks [21, 37].

5.3.2 Reducing Anonymity of Exchanges

Anonymity is a beneficial feature of online cryptocurrency exchanges that conceal the identities of their users, but it comes with a cost for exchange owners, especially as the lawful use of cryptocurrencies becomes increasingly more acceptable. Legitimate users may be hesitant to transfer funds or do business with an unregistered or untraceable and therefore unaccountable exchange.

In addition, anonymity limits an exchange's ability to increase and maintain its client base. It may also cause civil and criminal liability issues for the exchange and its owner if the exchange is required to be registered and transparent with its users. Therefore, exchanges and users may insist on KYC before conducting transactions. Some cryptocurrency exchanges have taken it upon themselves to register as MSBs, while others have been lobbying for legislative action on regulating the cryptocurrency market [11, 13].

5.3.3 Tracking Activities of Registered Exchanges

Even if a registered exchange frequently uses multiple public addresses or privacy browsers for concealment and can successfully communicate these addresses to its clients, authorities could track transaction histories to ascertain cryptocurrency amounts and suspicious activity since the addresses are public. Although the identities of the exchange owner or users may not be discoverable, authorities could use technology and still seize or suspend any suspicious accounts within the exchange or close the exchange entirely [37]. Furthermore, exchange owners and users eventually use more traditional routes to launder their funds, thereby converting cryptocurrency for fiat currency at a traditional exchange or with another entity not connected to a computer network. If this cash-out strategy occurs, identifying information will have to be provided to the financial intermediary, and any suspicious activity or money laundering red flags during such a transaction will have to be documented and reported.

While using an unregistered exchange, owner or user mistakes or inexperience during the cashing out process may lead to data leakage and providing authorities with trace evidence [13, 21]. Such mistakes can be as simple as using the same address or password for multiple purposes or accounts, not using privacy-preserving tools, providing a valid email address, or other security lapses. Some of these mistakes can happen while using a mixer/tumbler service provider or a TOR-enabled Dark Web site, as was the situation with the Silk Road case [37].

Thus, instead of increasing regulations or targeting cryptocurrency senders, receivers, processors (miners), or underground exchanges, the more effective regulatory approach regarding cyber laundering may be the targeting of:

1. Legitimate exchanges that swap cryptocurrencies for fiat currency [11, 37]
2. The physical locations of legitimate exchanges where human contact is most likely to occur
3. Classifying such businesses as money transmitters subject to the appropriate regulations required of money transmitters, such as filing CTRs and SARs [26, 37]

All these approaches have merit as legal exchanges are easier to regulate. Focusing regulatory efforts on them may also serve as a deterrent for money launderers to use shadow exchanges as the cost and risk could be significantly higher than the benefit. In 2015, the Financial Action Task Force (FATF), which is an international body focused on anti-money laundering, provided guidance to that effect and stated that countries should closely monitor exchanges that "send, receive, and store" cryptocurrency since such exchanges can be prime targets for cyber laundering. The FATF also stated that exchanges on their own should perform KYC and CDD to avoid anti-money laundering conflicts. The FATF further advised that exchanges found in violation of anti-money laundering regulations should be met with enhanced criminal, civil, and/or administrative punishments and ultimately prohibition of exchange activity [46].

However, none of these approaches constitute a robust regulatory solution against cyber laundering. Launderers may just be forced to avoid using cryptocurrency early in the laundering process or use more traditional exchange approaches to obtain fiat currency for cryptocurrency.

5.3.4 Regulating Cryptocurrencies

Another nontechnical solution would be to regulate cryptocurrencies. The regulation could range from a complete ban on cryptocurrency [26, 48, 49] to the legal recognition of cryptocurrency. Approximately one hundred and eleven countries take the latter approach, while some countries take the former. Other countries take a restrictive approach and prohibit the trading or use for cryptocurrency payment, while China, for example, completely bans cryptocurrency exchanges. Numerous other countries have been "undecided" because cryptocurrency is neither illegal nor legal, meaning that although owning cryptocurrency is legal per se, there are no legal protections or rules concerning its status or use. In general, countries seem to fall under two categories, either currently developing legal cryptocurrency frameworks or waiting to see its evolution.

At the same time, not all countries that legally recognize cryptocurrency have strict anti-money laundering laws against using cryptocurrencies in money laundering. The USA, Canada, the UK, Australia, and the member nations of the European Union (EU) have anti-money laundering laws applied to cryptocurrency.

The EU prohibits member countries from creating and introducing their own cryptocurrency, while cryptocurrency exchanges are urged to remain legal by complying with regulations [48]. Within the USA, the federal government could invoke the Commerce Clause (Article I, Section 8, Clause 3) of the Constitution to regulate the cryptocurrency market [11] explicitly.

The specific clause gives the US Congress the enumerated power of regulating commerce with foreign nations, among states, and with Indian tribes. Since cryptocurrency is frequently used to buy and sell goods and services and to exchange fiat currency through interstate trade, it may be possible for Congress to legislate the use of cryptocurrency directly. Some countries, such as Canada, China, Russia, Singapore, South Korea, and the UK and their central banks are considering developing and implementing their government-backed state cryptocurrencies to compete or replace existing cryptocurrencies by decree. Another reason for developing a state-sponsored cryptocurrency is the eventual abolition of cash so that transactions are better monitored for improved security and the elimination of tax evasion [46].

5.4 Technical Regimes Against Cyber Laundering

The main advantage for cyber launderers of using cryptocurrency is anonymity and decentralization. These two inherent characteristics of cryptocurrency make it difficult for authorities to trace and regulate its use and identify launderers. Some technical controls can be implemented to serve as deterrents for money launderers, but realistically, they are both technically and practically challenging to implement at scale.

5.4.1 Tracking IP Addresses

Even when an illicit actor uses a privacy-preserving application, such as the Tor browser, authorities may still be able to partially track IP addresses. Tolls exist, like the Exonera TOR tool that retains a database of past and current TOR network-linked IP addresses. It allows discovering if a TOR relay had been used by a particular IP address on a specific date. Even though the originating IP address will still not be discoverable, authorities can see if a suspect IP address under investigation matches any IP address listed on the tool's exit relay list.

Generally, tracking IP addresses may be helpful for cases that illicit actors may be inexperienced using privacy preservation tools and make mistakes during their use. An example would be using applications or generating not concealed or unreported network traffic due to the improper installation of browser plugins, the use of clear text over HTTP, allowing cookies, or running certain types of applications. These are possible technical mishaps that could be subject to computer forensic methods to discover an individual's identity.

5.4.2 Tracking the Blockchain

Because various cryptocurrencies utilize blockchain technology as a public ledger of transactions, public keys are used to represent users pseudonymously [10, 21]. Although public keys are changed frequently from transaction to transaction, blockchain's public nature allows for a more effective and more straightforward analysis process and recognition of patterns. Furthermore, it is nearly impossible to manipulate the data contained within a blockchain without incurring high costs due to its distributed nature. Therefore, there is a high degree of confidence that the data stored within a blockchain have been unchanged [22].

Since blockchain is a chain of transaction ownership where each transaction is dependent on the prior transaction, examination of the blockchain with a tool such as blockchain.info is possible and permits the verification that specific public keys sanctioned certain transactions or IP addresses [28]. Blockchain transactions are traceable, immutable, and irreversible [35, 50], allowing authorities to use the blockchain and its transaction histories for investigative purposes, rove illicit activity, or infer social ties between users [5]. To do so, blockchain transaction examination using extensive data mining and qualitative and quantitative analysis is necessary [10, 46]. An immutable audit trail can be established by carefully examining a blockchain's past and present transaction data, and essential information and significant patterns may be deduced, leading to user IP addresses or transactions being deanonymized [22, 46, 50].

Additionally, behavior analysis and heuristics can be performed on public keys frequently during payment [20, 21, 28]. By associating specific public keys to transactions, public key/transaction pairs can be developed across datasets and the network allowing the cluster mapping of behavior patterns and leading to the possible discovery of specific network users. These patterns can formulate a picture about a user's shopping and spending habits and frequency of transactions and go as far as identifying geographical locations. These patterns may potentially connect to third-party transactions, which may be associated with PII that authorities can use.

An interesting example of performing a trace that leads to an IP address was conducted using Bitcoin's [51] P2P network. Researchers could map public keys to IP addresses and eventually identify a Bitcoins user's IP address by analyzing Bitcoin's handshake protocol by exploiting the TPC/IP network-level protocol. Since each node within the Bitcoin system executes network routing to propagate addresses and must discover at least one other peer node established on the network to operate and distribute information, the nodes through port 8333 perform the handshake protocol over TCP. The handshake is initiated by the nodes exchanging messages and transmitting their presence via a simple message. This message contains the software version and block count. If a peer node can connect another node to the network, the peer node transmits a *verack* message back to the connecting node. Further research conducted by the researchers showed that the use of a Tor proxy prohibited their mapping of public keys and IP addresses and that use of a firewall or VPN to shield an IP address allowed them only to discover the Internet Service Provider (ISP) of the originating transaction [28].

6 Conclusion and Future Work

Traditional money launderers that engage in the cleansing of physical currency face a high degree of exposure risk and multiple possible points of failure. To avoid detection, they engage numerous associates as participants to repeatedly distribute, reroute, invest, and deposit illicit physical funds across multiple financial intermediaries or "invest" them in different assets and financial instruments. Even one failure during any of the multitude of these transactions may lead to detection by regulatory or law enforcement authorities and tracing of both the illicit funds and the original criminal activity that made them available.

The ease by which the Internet allows for the quick and easy transmission of data across jurisdictions, combined with the anonymity provided by cryptocurrency and blockchain technologies, has enabled traditional money laundering to transition into cyberspace. These risk and failure points are also present during cyber laundering, but significantly fewer. With cyber laundering, exposure risk and multiple points of failure are significantly reduced since most transactions can be completed anonymously online using commonly available privacy applications. Furthermore, money launderers in cyberspace do not have to rely on multiple associates that could make mistakes or get apprehended during the commission of their money cleansing tasks. Instead, cyber launderers can directly use an unregistered cryptocurrency exchange, transform fiat currency into cryptocurrency, and then use mixing/tumbler services to "clean" the cryptocurrency and further anonymize the transaction.

As law-abiding entities and organizations recognize and accept cryptocurrency for goods and services, the use of cryptocurrency by illicit actors will likely increase. Aside from those that fall victim to fraud, such an increase will pose additional security challenges to those responsible for anti-money laundering enforcement and regulation. Since cryptocurrency is a relatively new phenomenon within the money laundering scheme, most law enforcement, judicial, legislative, and private entities are inadequately prepared and equipped to handle cyber laundering cases. Furthermore, the legal definition and interpretation of cyber laundering and what it entails vary across jurisdictions resulting in confusion and ineffectiveness during cross-border cooperation and inconsistency in enforcement and regulatory efforts. These legal and financial systems shortcomings enable criminal organizations and cyber launderers to continue their money laundering practices.

It is perhaps typical that the legal and regulatory frameworks relating to cryptocurrency and blockchain are lacking globally. When the first cryptocurrencies entered the financial market, government entities worldwide ignored or refused to consider classifying cryptocurrency as a form of money or currency for legislative and legal purposes. The challenge and resulting confusion were due to the failure of these entities to recognize that instruments such as "digital coins" could have any value in the traditional sense of a currency. Most of these entities viewed the creation and issuance of legal tender as the exclusive right of governments [26, 45]. Before cryptocurrencies, the right of governments to control and issue legal tender, thereby protecting trade, was centuries old and practically unquestionable.

Case in point, the right of the British Crown to issue legal tender was affirmed by the English courts in 1605 and was so vital that it was also expressly given to the US government during the ratification of the US Constitution [40, 45]. Having a decentralized, autonomous, and unregulated currency would have been unfathomable. This mindset by governments worldwide has delayed long enough to engage, understand, and deliberately address cryptocurrency rather than letting the technology spread and grow uncontrollably. As of 2021, there are approximately 4737 cryptocurrencies within the cryptocurrency market, with a total global cryptocurrency market capitalization for the total circulating supply of cryptocurrencies at approximately $2.07 trillion [25].

This work examined the evolution and transition of traditional money laundering into cyberspace to become cyber laundering. We identified the technology and the regulatory challenges of detecting and enforcing the law under these new money laundering conditions. There is much work to be done on every front to fight cyber laundering, but demonizing anyone besides those that engage in cyber laundering would be a mistake.

It would also be a mistake to demonize these new algorithms and technologies that support the mining, storage, and exchange of cryptocurrencies. As with any evolving technology, cryptocurrency and blockchain are beneficial and innovative technologies for lawful and nefarious purposes. They can revolutionize how business is conducted and positively impact and transform national and international economies if regulated and appropriately used. Governments and enforcement agencies will ultimately decide upon a regulatory approach to the use of cryptocurrency. Hopefully, their legislative approach will be balanced, precise, and targeted but not overly burdensome to lawful consumers of such a product. It also should be an international collaborative effort to implement regulatory uniformity among varying jurisdictions. Furthermore, it should be flexible enough to foster future technological innovation and growth of payment systems and the global market.

References

1. C. Pacini, N.F. Stowell, I.J. Katz, G.A. Patterson, J.W. Lin, An analysis of money laundering, shell entities, and no ownership transparency that washes off and on many shores: a building tidal wave of policy responses. Kansas Journal of Law &Public Policy **30**, 1 (2020)
2. K.J. McCarthy, Who Runs the Laundry?, in *The Money Laundering Market*, ed. by K.J. McCarthy. Regulating the Criminal Economy (Agenda Publishing, New York, 2018), pp. 33–54
3. P. Reuter, E. Truman, How much money is laundered?, in *Chasing Dirty Money: The Fight Against Money Laundering*, Illustrated edn. (Peterson Institute for International Economics, Washington, DC, 2004), pp. 9–24
4. W. Filipkowski, Cyber Laundering: An Analysis of Typology and Techniques. Int. J. of Criminal Justice Sci. **1**, 15–27 (2008)
5. C. Brenig, R. Accorsi, G. Müller, Economic analysis of cryptocurrency backed money laundering, in *ECIS* (2015), pp. 1–18

6. S. Turner, U.S. Anti-Money laundering regulations: an economic approach to cyberlaundering. Case West. Reserv. Law Rev. **54**, 1389 (2004)
7. J. Hunt, The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them. Inf. Commun. Technol. Law **20**, 133–152 (2011)
8. A. Krishnan, Blockchain empowers social resistance and terrorism through decentralized autonomous organizations. Journal of Strategic Security **13**(1), 41–58 (2020)
9. D. Bryans, F.J. Anema, Bitcoin and money laundering: mining for an effective solution, in *The Money Laundering Market*, ed. by K.J. McCarthy. Regulating the Criminal Economy (Agenda Publishing, New York, 2018), pp. 139–170
10. D.B. Desmond, D. Lacey, P. Salmon, Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. Journal of Money Laundering Control **22**, 480–497 (2019)
11. S.D. Hughes, Cryptocurrency Regulations and Enforcement in the U.S. W. St. U. L. Rev. **45**, 1 (2017)
12. A. Turner, A.S.M. Irwin, Bitcoin transactions: a digital discovery of illicit activity on the blockchain. J. Financial Crime **25**, 109–130 (2018)
13. R. van Wegberg, J.-J. Oerlemans, O. van Deventer, Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. J. Financial Crime **25**(2), 419–435 (2018)
14. J. Cassara, *Money Laundering and Illicit Financial Flows: Following the Money and Value Trails* (2020)
15. United Nations Office on Drugs and Crime, in *Money Laundering*. https://www.unodc.org/unodc/en/money-laundering/overview.html. Accessed: 2021-03-18
16. PwC, PwC's Global Economic Crime and Fraud Survey (2020). https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html. Accessed: 2021-03-18
17. J.B.a. Sykes, *Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals*, Library of Congress public edn. (Congressional Research Service, Washington, D.C., 2018)
18. J.R. Richards, *Transnational Criminal Organizations, Cybercrime, and Money Laundering: Handbook for Law Enforcement Officers, Auditors, and Financial Investigators* (1999). OCLC: 4769468015
19. P. Reuter, E. Truman, Chasing dirty money, in *Chasing Dirty Money: The Fight Against Money Laundering*, illustrated edn. (Peterson Institute for International Economics, Washington, DC, 2004), pp. 1–8
20. A.S. Irwin, A.B. Turner, Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. Journal of Money Laundering Control, vol. 21, 297–313 (2018)
21. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2009). Cryptography Mailing list at https://metzdowd.com
22. Katarzyna Ciupa, Cryptocurrencies: Opportunities, Risks and Challenges for Anti-Corruption Compliance Systems (2019). Presented at the 2019 OECD Global Anti-Corruption and Integrity Forum, Paris, France. https://gacif2019.sched.com/artist/katarzyna_ciupa.1z9t5alt. Accessed: 2021-12-27
23. Cryptocurrency Prices, Charts and Market Capitalizations. https://coinmarketcap.com/. Accessed: 2021-03-01
24. M. Conti, A. Gangwal, S. Ruj, On the economic significance of Ransomware campaigns: a bitcoin transactions perspective. Comput. Secur. **79**, 162–189 (2018). arXiv: 1804.01341
25. K. Singh, The new wild west: preventing money laundering in the Bitcoin network. Northwest. J. Technol. Intellect. Prop. **13**, 37 (2015)
26. A. Berentsen, F. Schar, A short introduction to the world of Cryptocurrencies, in Economic Research, Federal Reserve of St. Luis. https://research.stlouisfed.org/publications/review/2018/01/10/a-short-introduction-to-the-world-of-cryptocurrencies. Accessed: 2021-04-11
27. M. Levi, P. Reuter, Money Laundering. Crime Justice **34**, 289–375 (2006)

28. V. Dyntu, O. Dykyi, Cryptocurrency in the system of money laundering. Baltic Journal of Economic Studies **4**, 75–81 (2018)
29. M. Campbell-Verduyn, Bitcoin, crypto-coins, and global anti-money laundering governance. Crime Law Soc. Chang. **69**, 283–305 (2018)
30. Internal Revenue Service (IRS), Money Laundering and Currency Crimes. https://www.irs.gov/irm/part9/irm_09-005-005. Accessed: 2021-12-27
31. K.-K.R. Choo, Chapter 15—Cryptocurrency and virtual currency: corruption and money laundering/terrorism financing risks?, in *Handbook of Digital Currency*, ed. by D. Lee Kuo Chuen (Academic Press, San Diego, 2015), pp. 283–307
32. N.D. Bhaskar, D.L.K. Chuen, Bitcoin Mining Technology, in *Handbook of Digital Currency*, ed. by D. Lee Kuo Chuen (Academic Press, San Diego, 2015), pp. 45–65
33. L. Ante, Cryptocurrency, Blockchain and Crime, in *The Money Laundering Market: Regulating the Criminal Economy* (Agenda Publishing, New York, 2018), pp. 171–198
34. D. Yermack, Chapter 2 - Is Bitcoin a real currency? an economic appraisal, in *Handbook of Digital Currency*, ed. by D. Lee Kuo Chuen (Academic Press, San Diego, 2015), pp. 31–43
35. U.S. Constitution—Art. I, Sec. 8, Cl. 3. https://constitution.congress.gov/constitution/article-1/. Accessed: 2021-12-23
36. C. Albrecht, K.M. Duffin, S. Hawkins, V.M. Morales Rocha, The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control **22**, 210–216 (2019)
37. S. Middlebrook, S. Hughes, Regulating cryptocurrencies in the United States: current issues and future directions. William Mitchell Law Review **40**, 813 (2014)
38. Lauren Troeller, Bitcoin and Money Laundering, in *Boston University—Review of Banking and Financial Law, no. Issue I – Fall 2016* (2016), pp. 159–174
39. G. Weimann, Going dark: terrorism on the dark web. Studies in Conflict & Terrorism **39**, 195–206 (2016)
40. C. Jaag, C. Bach, Chapter 6—the effect of payment reversibility on E-commerce and postal quality, in *Handbook of Digital Currency*, ed. by D. Lee Kuo Chuen (Academic Press, San Diego, 2015), pp. 139–151
41. U.A. Zanconato, The shadow banking system, in *The Money Laundering Market*, ed. by K.J. McCarthy. Regulating the Criminal Economy (Agenda Publishing, New York, 2018), pp. 89–112
42. P. Verschuuren, Money laundering, sports betting and gambling, in *The Money Laundering Market*, ed. by K.J. McCarthy. Regulating the Criminal Economy (Agenda Publishing, New York, 2018), pp. 113–136
43. S. Dyson, W.J. Buchanan, L. Bell, The challenges of investigating cryptocurrencies and blockchain related crime. The Journal of the British Blockchain Association **1**, 1–6 (2018). arXiv: 1907.12221
44. S. Mabunda, Cryptocurrency: the new face of cyber money laundering, in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (2018), pp. 1–6
45. S. Berg, K.J. McCarthy, An introduction to the challenges of money laundering, in *The Money Laundering Market*, in K.J. McCarthy. Regulating the Criminal Economy (Agenda Publishing, New York, 2018), pp. 3–32
46. FinCEN.gov, What is money laundering?. https://www.fincen.gov/what-money-laundering. Accessed: 2021-11-01
47. Jerry Brito, Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies, Testimony Before the Senate Committee on Homeland Security and Governmental Affairs (2013). https://www.govinfo.gov/content/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf. Accessed: 2021-04-13
48. Countries Where Bitcoin is Banned or Legal (2021). https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm. Accessed: 2021-11-23
49. N.C.C. Sugimoto, Anastasiia Morozova, Regulation of Crypto Assets. https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Regulation-of-Crypto-Assets-48810. Accessed: 2021-11-01

50. Federico Paesano, Working Paper 28: Regulating Cryptocurrencies: Challenges and Considerations, in *Basel Institute on Governance*. https://baselgovernance.org/publications/working-paper-28-regulating-cryptocurrencies-challenges-and-considerations. Accessed: 2021-11-23
51. M. Möser, R. Böhme, D. Breuker, An inquiry into money laundering tools in the Bitcoin ecosystem, in *2013 APWG eCrime Researchers Summit* (2013), pp. 1–14
52. C. John, Money Laundering and Illicit Financial Flows: Following the Money and Value Trails, in *Money Laundering and Illicit Financial Flows*

Part V
Blockchains in Education, Governance, Supply Chain, and Security

A Blockchain-Based Fair and Transparent Homework Grading System for Online Education

Cheng Ting Tsai and Ja Ling Wu

1 Introduction

Blockchain is a chronologically ordered data structure with decentralization, trustworthiness, and group sharing as its most attractive features. The popularity of Bitcoin [1] proved that blockchain techniques contribute to the stability and liveliness of a massively distributed system, where data and executive activities are decentralized, supervised, and maintained by all chain members, which, in turn, makes the interaction between each other fair, secure, and transparent. The above facts explain why blockchain has been successfully applied to various fields, such as medicine, profit sharing, finance, etc., where all involved members should be treated equally, or the legitimacy of information transfer must be considered seriously. Among those applications, education is the one which impacts everyone for life and is one of the crucial keys for leading to today's rapid technology development. Although the spread of the epidemic has put the discussion and debate about virtual education in the spotlight, this topic is not new; teaching and learning have been in various virtual formats for years. COVID-19 pandemic turbocharged the move from physical education and learning to online forms; instead of creating a new trend, it has merely accelerated something already underway.

C. T. Tsai
Department of Electrical Engineering, National Taiwan University, Taipei City, Taiwan

J. L. Wu (✉)
Department of Computer Science and Information Engineering, National Taiwan University, Taipei City, Taiwan

Graduate Institute of Networking and Multimedia, National Taiwan University, Taipei City, Taiwan
e-mail: wjl@cmlab.csie.ntu.edu.tw

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_13

For example, massive open online courses (MOOCs) [2] have been brought to public notice recently. Originated from the USA, MOOCs are developed by leading content providers like Coursera, Udacity, and edX [3]. Since 2012, top American universities have been setting up online learning platforms and offering free online courses. Targeting higher education, MOOCs are featured by quality teaching programs and independent management systems. National Taiwan University (NTU) is especially delighted to join other world-class universities on Coursera and offer quality university courses to the Chinese-speaking population [4]. Despite the worldwide popularity, the current online education systems have many shortcomings in the face of the untrustworthy Internet. Most often given criticisms of MOOCs include [5]:

1. The learning process and results of MOOCs are short of public recognition and official certification.
2. The students' privacy is at risk, for the courses and data security solely depend on the centralized online education platform.
3. The educators' and students' intellectual properties are hard to be maintained effectively due to the openness of the Internet and the vulnerability of data.
4. There is no mature cross-platform to share the teaching resources fully.
5. To make the learning process and results trustable, it is necessary to develop a distributed and trustable data storage method to record the students' learning process, disclose all learning data to the public, and ensure the security and non-vulnerability of data.

Blockchain seems almost tailor-made to help secure and protect this new education model with a combination of information security and the ability to share this data among an open network of counterparties and do so in a completely online manner [6].

Nowadays, many problems exist in online educational platforms since the correlation and interaction between students and teachers are not reciprocally equal; additionally, only a few administrative members possess the right to supervise the on-platform activities. This often results in misunderstanding, unnecessary conflicts, and, the worst, various forms of misbehavior among students and teachers, such as post-grade cheating and discriminative grading, for their benefit. Discriminative grading means a teacher is retreating course-related announcements which are currently guiding their decision and grading different students with different standards. Post-grade cheating says a student changes their answer after the assignment's correct solution has been released to ask for more scores. Clearly, if the on-platform activities are not trackable, the system may not be confident enough in ensuring fair and trustworthy teacher–student interactions. Another common challenge in homework grading is grading an open-ended question, which allows different kinds of opinions as to the answers, such as essay questions or calculation problems. Students usually argue that the teacher did not understand what they were trying to express, which is reasonable since none can consider or accept all possible views to a question. Thus, grading this kind of answer by just one person is not convincing, and controversies often occur, especially when the score is very crucial, for example, the score of essay exam in English proficiency test. Usually, fairness can be achieved only when it is a large-scale examination and multiple judges are recruited to do the grading. Even so, judges are more or less affected by others' opinions, especially when they are familiar with each other (which is, in fact, an often case).

In facing this issue, we proposed a blockchain-based homework grading system to establish a fair and transparent teacher–student interaction platform. On-chain members are anonymous, and their interactive activities are immutably trackable. Our work was built based on the Ethereum architecture, with the aid of multiple Cryptographic algorithms, to prove its feasibility and applicability. When all on-chain members are treated equally, we believe the proposed approach will somewhat release the following downsides in gradings, such as discriminative grading by teachers, post-grade cheating between students and teachers (or teaching assistances [TAs]), and the divergence grading for open-ended questions. A mechanism to allow teachers to uncover the identities of anonymous students, which will be activated only at the end of the course, is also introduced to correctly give the final scores to the corresponding students. Moreover, three autonomous smart contracts are designed to guarantee fairness and efficiency in homework correction work, which helps reduce teachers' loads essentially. Finally, this work also focused on the system implementation issues; therefore, some applications constructed based on our system will be presented, and the corresponding operational experiments are also provided.

In short, by combining blockchain, smart contract, and some cryptographic algorithms, this work tries to build a trustworthy teacher–student interaction platform. The platform is suitable for many kinds of correction works, such as homework assignments and exam papers. Our goal is to encourage students to learn the right attitudes and correct approaches during their study phase by providing an equal opportunity guarantee in their score grading process.

2 Related Work

2.1 Blockchain

Blockchain can be viewed as a combination of multiple technologies, such as network security, information transmission, distributed database, cryptography, etc. As a distributed system, nodes on a blockchain network reach a consensus by a designed protocol. Proof of work (PoW) [7] is the most well-known one among many different consensus protocols. A miner verifies every transaction before being put into a block; every node that receives the block will prove the existence and legality of the associated transactions again. Blockchain uses a specific data structure, aka Link List or Directed Acyclic Graph (DAG) [8], to store and to chain verified transactions. This implies every transaction is immutably trackable in a blockchain. Each block contains a block header that records the block's information, such as timestamp, the difficulty of PoW, etc. Additionally, a previous-block-header hash, which is the hash of the previous block header, is also included. Therefore, changing any information within a block will result in a different previous-block-header hash from the one recorded in the next block. Suppose one wants to alter a piece of on-chain details, such as the contents of transactions in a block. In that case, they have to change all connected blocks behind the target block, which is a highly time-consuming task and is almost impossible to achieve under a well-designed consensus algorithm. Every active account can watch and supervise the activities of every other account and will have a backup of its data in the blockchain. A part of on-chain nodes that failed or lost their data will not cause the system to malfunction; instead, failed nodes can repair their losses through data synchronizing mechanism with the other nodes.

Activities in a blockchain are trackable, but it doesn't mean that there is no privacy for users. A user joined in a blockchain is represented as an on-chain account. Others can see the account's activity and verify its transactions but will never know who actually owns the account. Finally, a set of cryptographic algorithms, an indispensable part of a blockchain, is used to realize most blockchain properties, such as verifying the legality of transactions, generating valid public and private keys, and encrypting sensitive information. Commonly adopted cryptographic algorithms for supporting these purposes include SHA256 secure hash, Elliptic Curve Digital Signature Algorithm (ECDSA) [9–11], and keccak256. Cryptographic mechanisms can also help on-chain nodes prove the existence of transactions efficiently without requiring storing the raw data of all the related transactions. This makes devices with limited storage workable as a lightweight node of a blockchain, for example, the Simplified Payment Verification (SPV) node in Bitcoin.

2.2 *Blockchain in Educations*

Blockchain can be used to carry and transfer any valuable assets, such as currency, copyright, knowledge, and records. There is much helpful information in education, including research data, experimental documents, scores, credits, and certificates of degrees that are extremely important for both students and educators, where management, security, and fairness are necessary and of importance. Thus, blockchain is a suitable vehicle to bring benefits to educations [12–15] and makes management of all the students' and educators' information reasonably, especially for online education platforms. As pre-described, in the well-known and widely adopted MOOC platform, students and educators have come from different places of the world to achieve their own goals in education. Clearly, establishing trust between each member in such an assortment and diverse education environment becomes very challenging.

In recent years, there have been researching works focused on using blockchain to manage, share, and verify degrees [16, 17], research results, and data [18]. However, most of the works focused on managing a higher layer of information in education, for example, recording and sharing students' certificates and degrees between colleges. Some of them only explained concepts or discussed potentials for the future. In contrast, our work realized a design that aims to manage some lower-layer information of education, that is, teacher–student interactions, homework assignments, and grading in courses to ensure that a student gets his credits and completes his degrees transparently and fairly.

Blockchain provides students an easy way to store and manage their credits and degrees while allowing educators, universities, and institutions to manage student-related affairs, share their information with other universities, and track their learning histories and outcomes. It can also prevent improper activities, such as cheating or forgeries. With the aid of blockchain, every move can be verified and supervised by all involved members. With blockchain, a student can apply for the entrances to colleges without printing a mass of diplomas or certificates of programs learned; instead, colleges can find the student's information, including records and degrees, or even comments to this applicant from responsible teachers, directly. This will save resources and time and establish fairness, transparency, and security of information flow.

2.3 The Ethereum

Ethereum [19, 20] is one of the blockchain architectures introduced between 2013 and 2014, devoting to establish a global and most completed blockchain system. Ethereum is very popular and considered to be a considerable breakthrough in blockchain development. One of the crucial contributions of Ethereum is its involvement of smart contract, a computerized transaction protocol executing the terms of a contract, which is written by a specific programming language, such as Solidity [21]. Smart contracts can be independently and autonomously executed by nodes on an Ethereum network using virtual machines, the Ethereum virtual machines (EVMs) [19]. The Turing completeness of smart contract allows Ethereum blockchain to be applied to many complex tasks, such as funding, supply chaining, bidding, and even signing another contract. This makes blockchain no longer be a purely distributed system that can only send transactions, instead a completed decentralized architecture for transferring virtual currencies. Ethereum is also open sourced so that everyone can join and research on it or build their own designed private Ethereum-based chains. Therefore, if one wants to develop a blockchain system to fulfill some complex use cases in which smart contract may be necessary, Ethereum is one of the best platforms for development. In light of this fact, our work is also realized based on the Ethereum architecture.

3 Preliminary and Basic Definitions

3.1 Computational Power

In the proposed work, the computational power is assumed to be uniformly distributed to all involved members. Each member joins the consensus mechanism and has an equal chance and responsibility to create a new block and maintain the liveness of the system. Some members may have better computational power than others, and we assumed they would not gather enough computational power to conspire against or even sabotage the system.

3.2 Regulations and Accounts

Our design focuses on the most fundamental aspect of education: the teacher–student interactions in a course to establish a fair, open, and secure assignment/grading system. Therefore, this work is expected to operate correctly under the supervision of an educational institution or online platform, where regulations are made to restrict both students and teachers from sabotaging the system. This may seem to centralize the system; however, the system's operations are designed not to interfere with the administrator. This means the system is decentralized execution by the students and teachers, and of course, they have to follow the regulations supervised by the administrator. On the other hand, the administrator has to verify the validity of statuses of students and teachers after they signed in the system and intervenes between students and teachers only when some disputes against the preset rules occur.

In each quarter or semester, every qualified member, such as teacher, student, and teaching assistance, will respectively receive an address, which points to the corresponding account used in the assignment/grading system, from the administrator. After registration, the administrator gives teachers their student lists. The list contains the student accounts associated with the enrolled members of the corresponding classes (to prevent non-registered students from joining the courses without permission) and the students' IDs to identify the students who did take the courses at the end of the quarter/semester (c.f. Sect. 4.4 for details). Notice that the correspondence between accounts and students' ID has remained in secret (c.f. Fig. 1). That is, the teacher will never know which student owns the specific account until the course is finished. The administrator uses the accounts to track and supervise members' behaviors to enhance the stability and liveliness of the system. Offenders are suspended or punished according to the regulations or even laws depending on the severity of disobedience.

Supervisions and regulations are a must to make the system highly reliable and functional. However, the system will still operate in a decentralized manner due to the nature of blockchain. Once the system starts, it will be maintained and

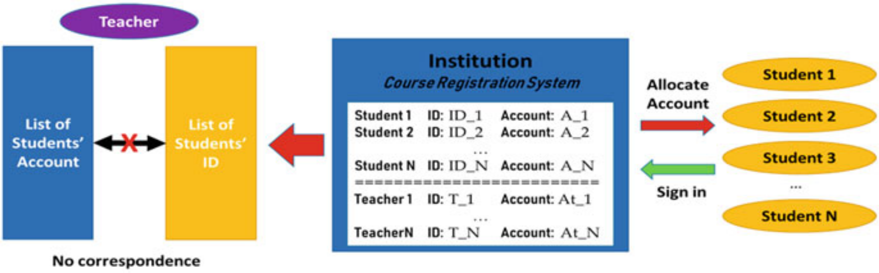

Teacher
List of Students' Account
List of Students' ID
No correspondence
Institution
Course Registration System
Student 1 ID: ID_1 Account: A_1
Student 2 ID: ID_2 Account: A_2
...
Student N ID: ID_N Account: A_N
Teacher 1 ID: T_1 Account: At_1
...
TeacherN ID: T_N Account: At_N
Allocate Account
Sign in
Student 1
Student 2
Student 3
...
Student N

Fig. 1 Basic architecture and definition of the proposed system

verified by every on-chain member. It will be almost impossible to interfere with its operation or temper the data stored on it, even by the administrator.

4 The Proposed System

4.1 Basic Member Interaction Models

In every scenario of education, there is an interaction between students and teacher(s). Our simplest model aims at the interaction between students and teacher(s) through a blockchain architecture. The following three functional modules must be defined: homework assignment and submission, send grading results to students, and class information announcement. A teacher can assign homework or deliver announcement information to students by simply sending transactions with messages. On the other hand, by following the same principle, students can submit their homework; however, it does not make sense to put all messages (e.g., homework answers) directly on a transaction since blockchain is a transparent system. This is because every on-chain member can see the content of any validated transaction. In short, submitting homework in its plaintext form equals letting students share their answers with others. Therefore, messages that are not suitable to be publicized must be encrypted before sending them out. There are various ways to encrypt messages for securing transmitted data. In this work, the Rivest–Shamir–Adleman (RSA) algorithm [10, 22], one of the widely used encryption methods that is pretty easy to implement while very hard to be cracked, is applied. Thus, in our model (c.f. Fig. 2), the teacher needs to generate a key pair and send the public key to the students and the assigned homework. Students then encrypt their submission messages by RSA with the public key and send the ciphertexts of their respondent messages to the teacher. The messages include answers to the homework and the identity information of the student (c.f. Sect. 4.4) so that every student will generate a very different ciphertext even if their answers are the same and, thus, won't make plagiarism without being discovered. Finally, the teacher can restore the students' homework answers by decrypting the ciphertexts with the private key.

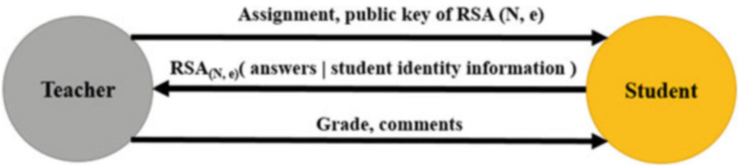

Assignment, public key of RSA (N, e)
RSA$_{(N, e)}$(answers | student identity information)
Grade, comments
Teacher
Student

Fig. 2 The interactions between teachers and students

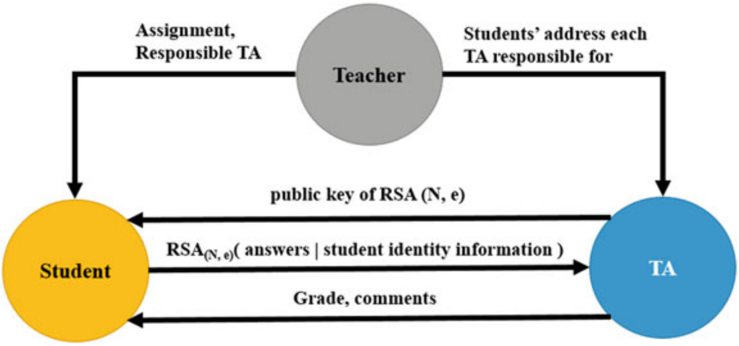


Fig. 3 The interactions among teachers, TAs, and students

By this approach, our system not only keeps the message secret but also prevents post-grade cheating. The process of this model is similar to that of the traditional online course platform; however, all students and teachers put their trust in this model, and every system player has fair rights and legal duties to maintain and interact with the model. All system activities are easy to be tracked and supervised; therefore, deleting or modifying any content of the announcement, assignment, and hand-in message in the working path is nearly impossible. In summary, this model uses blockchain to build a secure and fair online course platform, by which all members are encouraged to be responsible to themselves and to learn and to teach with the right attitudes.

4.2 The Role of Teaching Assistant

In every quarter/semester, teaching assistants (TAs) are often recruited to help distribute tasks and run a large-scale course. A TA's most often tasks are correcting term-in homework and examination papers. Thus, our model is extended to consider the interactions among students, TAs, and teachers. As shown in Fig. 3, the bottom half of the new model is similar to that of Fig. 2, where the only difference is that TAs now do the submissions' correcting task. In this case, a teacher still needs to assign homework to students, announce the responsible TA for each student, and give proof that the teacher genuinely released the assignment. On receiving the proven assignment or announcement, TAs and students interact with each other accordingly.

4.3 Collective Grading

In education, answers to the questions are not permanently fixed; in contrast, solutions are often opened to various opinions, such as essay questions. However, judging those kinds of answers by only one person is unfair because a person can't have all possible perspectives to a question. Even a teacher thinks the answers are very wrong; it does not mean that they are invaluable opinions. This is why there are often disagreements and conflicts with the grading of essay questions. Thus, to achieve better fairness in grading, scores should be given through various judges. This kind of multiple-person grading is called collective grading in this work.

Collective grading is done by extending the two models mentioned above. Students, the responsible teacher, and multiple judges (qualified professionals in the related fields) can join the correction process. The assignment (homework or exam paper) still needs to be given by the responsible teacher to prove its legality; however, students have to submit the ciphertexts of their answers to all judges, of course, including the responsible teacher. After the deadline, the responsible teacher shares the plaintexts of assignments, students' answers, and sometimes the teacher's remarks (optional) to other judges. In contrast, judges use the ciphertexts and the public key received from the responsible teacher to verify the plaintexts to ensure the plaintexts have not been tempered. Finally, judges will send their scores to the responsible teacher and corresponding students to calculate the final scores based on the preset weighting. The responsible teacher sends two scores to each student, one is the teacher's own giving score as a judgment, and the other is the final (collected and weighted) score sent to be recorded and verified. Once again, since messages are trackable in blockchain, forging scores or making teacher and student receive different scores becomes very difficult.

The timing for judges to receive the assignment containing homework or exam paper information is worthy of further discussion. The consideration is that the sooner the judges see the questions, the higher their chance to discuss with others and be affected when making judgments to students' answers. To prevent this shortage, judges should receive the contents of the assignment only when they are told to start the grading. However, this means that the responsible teacher cannot directly upload the plaintexts of assignments to students while announcing homework or exam papers; instead, the ciphertext of each assignment should be sent due to the transparency of the blockchain. As pre-described, uploading plaintext to blockchain equals sharing messages to all on-chain members, and an RSA key pair is required to avoid such a scenario. However, asking all students to generate their key pair with the responsible teacher is very inefficient because the teacher will do the encryption work the same number of times as the number of enrolled

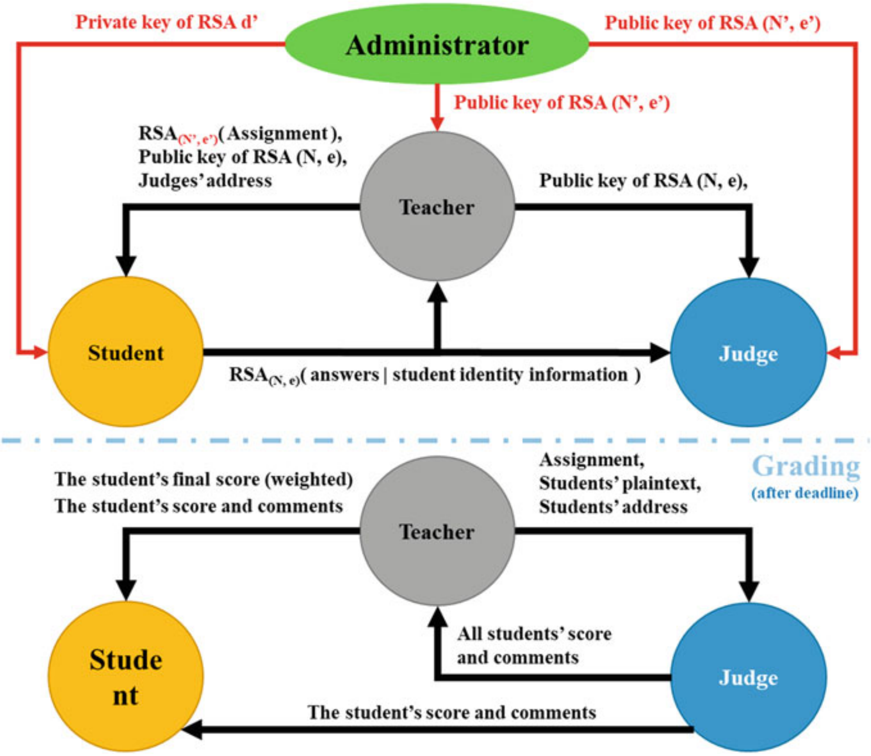

Private key of RSA d'
Administrator
Public key of RSA (N', e')
Public key of RSA (N', e')
RSA(N', e')(Assignment),
Public key of RSA (N, e),
Judges' address
Teacher
Public key of RSA (N, e),
Student
Judge
RSA(N, e)(answers | student identity information)
Grading
(after deadline)
The student's final score (weighted)
The student's score and comments
Teacher
Assignment,
Students' plaintext,
Students' address
Stude nt
All students' score
and comments
Judge
The student's score and comments

Fig. 4 Interactions among the responsible teacher, invited judges, and students in collective grading

students. Moreover, it is easier to make mistakes in facing such a complicated task. Therefore, our system administrator helps generate an RSA key pair beforehand for each student, sends the public key to the responsible teacher, and starts the judgment while giving the private key to the corresponding student. In this way, the responsible teacher can assign homework and exam papers with ciphertexts, and only the related student can decrypt them. Finally, the responsible teacher sends the plaintext of the assignment together with the students' answers to the invited judges when the grading work starts. Therefore, the judges can use the public key to verify and ensure the received plaintexts have not been tempered.

By this approach, homework or exam papers' grading outcomes with open answers will be more convincing. Additionally, the invited judges in this model (c.f. Fig. 4) can be anonymous so that each judge can grade the answers without being affected by others, which, therefore, can ensure the quality and fairness of their grading results more. Clearly, for extremely sensitive scores, especially those scores of crucial exams directly related to the certificates and the qualifications of the entrance, the method mentioned above is believed to be a reliable way for establishing credibility in grading.

4.4 Authentication

In a blockchain, every member's activity is anonymous by using an account to hide the user's true identity. In our words, this property allows students to take courses without giving up their privacy. It also ensures teachers equally treating their students by masking sensitive information such as students' IDs of each account. However, it brings problems when a teacher wants to give final grades to students because there is no idea which student owns the account. To deal with this challenge, Shamir's Secret Sharing algorithm [23] and Chaotic Cryptographic algorithms [24, 25]-based authentication schemes are introduced in this subsection.

At the beginning of the course, by using Chaotic Cryptography, each student generates their secret codes by encrypting their student ID with the chosen password and segments their secret codes into isolated pieces using Shamir's Secret Sharing algorithm (cf. Fig. 5). Students then send each of their private pieces together with their hand-in homework to the teacher to eventually find their secret codes out (cf. Fig. 6). The t-out-of-N, (N, t)-, Threshold Shamir's Secret Sharing algorithm is adopted, which initially segments the secret into N pieces. The secret can later be recovered exactly if at least t out of the N pieces are retrieved.

In our system, the parameter N is set to the total number of homework assignments in a course, and t is the least number of homework assignments that a student has to submit for getting the grade, which the teacher preset. Because it is nearly impossible for every student to submit every homework on time for some unpredicted reasons such as missing the deadline or not completing the assignment, the teacher should still recover the secret codes with only a part of hidden pieces. Additionally, stipulating the least number of must hand-in homework assignments may encourage students to learn and work harder is also a common practice. If a student fails to fulfill the minimum requirement, the teacher won't recover the secret codes for identifying them and, thus, no final score will be given to the student. In

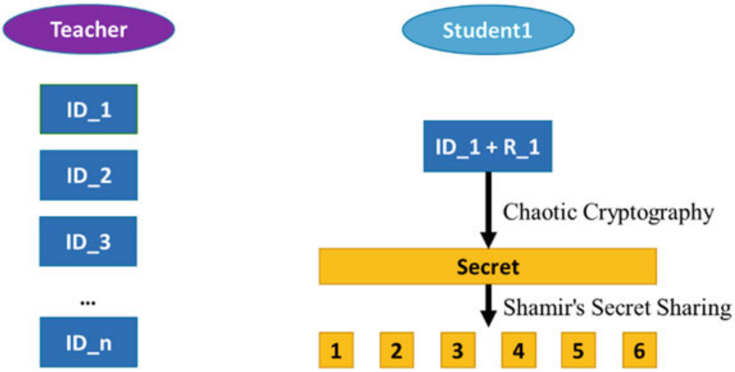


Fig. 5 Student generates secret codes and segments the codes into some secret pieces

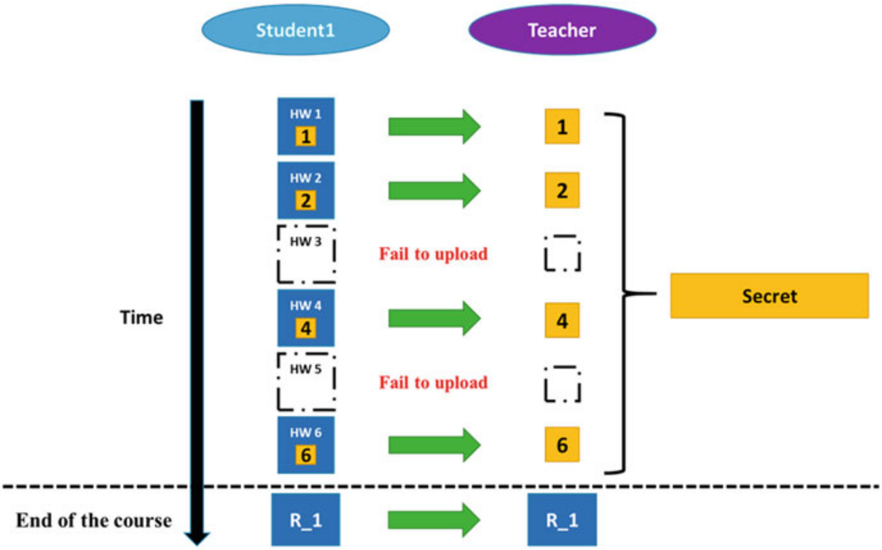


Fig. 6 Teacher recovers a student's secret codes by retrieving secret pieces sent together with the hand-in homework

contrast, if a student can prove their efforts put into the course, the final score should still be given even some of the submissions are missing or incomplete.

The integration with the Secret Sharing algorithm makes our system closer to the needs of real application scenarios; however, the adopted (N, t)-Threshold scheme also implies that the teacher can obtain the students' information far before the course is completed. That is why Chaotic Cryptography was applied earlier to play a crucial role in protecting students' privacy. A teacher can never find out the student ID within the secret codes without knowing the password set by the student. A student's identity will remain secret before the student sends out the final key information, that is, the password, to the teacher, at the end of the course (cf. Fig. 7). Additionally, since no student ID will be shared on the blockchain, a student's identity behind a given account is safe and remains unknown to the other members. By combining the above schemes, a teacher can identify the students enrolled in their course and set some rules (such as the values of N and t) for the course while privately setting passwords protects the students' privacy.

5 Smart Contract

As pre-described smart contract is a crucial feature of blockchain, using a designed protocol to decentralized and autonomously run-on networked nodes for achieving various complex tasks. Once deployed, a smart contract acts as a fair and transparent

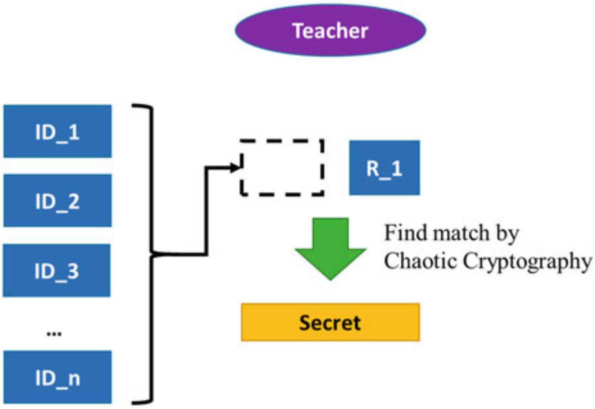


Fig. 7 Teacher identifies the first student with the password (R_1) and the associated secret codes

arbiter to deal with every request from its users. In educations, of course, there are many complex situations that smart contracts can be applied to make things easier. For example, it helps collect group lists or acts as a billboard to announce information. It is worth mentioning that a well-designed smart contract can also replace TAs for completing tasks that have clear regulations to follow, such as correcting homework or grading. Smart contracts guarantee tasks can be done truly impartially as comparing with TAs that may have specific personal opinions to certain students, more or less. Considering that scores are often the most critical basis of all credits, degrees, and certifications, three ways to grade homework or exams by smart contract are proposed in this section to ensure the grading is fair and transparent to every student. The first approach is to make students' grades by mutually exchanging the students' submissions. The second one is to grade the submissions by a smart contract automatically. Finally, the third is to grade students collectively, that is, using the smart contract version of Sect. 4.3.

Before getting into the details, an important mechanism must be introduced first. As mentioned in Sect. 4.1, sending answers in plaintext form equals sharing solutions to everyone in the blockchain before the deadline is reached, which is certainly not allowed. However, using a smart contract to decrypt a ciphertext is very difficult and costly due to the complexity of the involved deciphering algorithms. What's worse, uploading a private key to the blockchain has to pay the cost for storing large random numbers and reveals the private key to all on-chain members. Operationally, it is not easy to avoid making mistakes when embedding such a massive message into a transaction. Therefore, a better way to protect information security is to use the smart contract to directly verify the ciphertext with the aid of various commitment schemes instead of decrypting it back to plaintext and then doing the correction and grading tasks. When an assignment is announced, students need to upload their answers in ciphertext form before the deadline. The secure hash algorithm used to obtain the ciphertext should also be supported by the smart

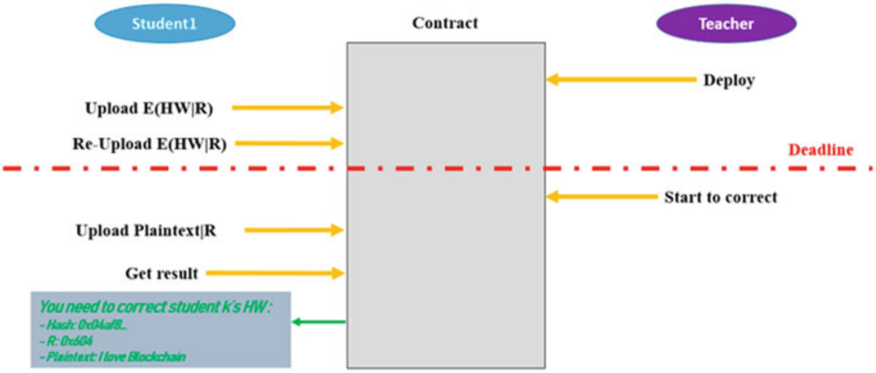


Fig. 8 Schematic diagram of smart contract-based grading by using mutual exchanging mechanism

contract to optimize the efficiency truly. The keccak256 hash algorithm, which is a callable function to Solidity language, is adopted in our work.

The same as in Sect. 4.1, the plaintext mentioned above should contain an extra message, denoted as R in Fig. 8. We use it to prove the student's identity at the end of the course and prevent the occurrences of post-grade cheating or homework-copying flaws by ensuring every student will get a unique hash value even if their answers are the same. After the deadline is reached, students upload their solutions together with message R, in plaintext, to the smart contract. The smart contract can prove the integrity of answers by checking if the plaintext's hash matches the ciphertext uploaded beforehand. Once the above answer is confirmed, then the plaintext of the solution can be directly graded manually by students or automatically by the smart contract.

5.1 Contract for Grading by Mutual Exchanging

A simple way to make the grading of each student's submission fair and efficient is to let students correct and grade the answers for each other, which is also a traditional way to correct homework or exam papers in junior and senior high schools. In the blockchain, no one can know the owner of each address. That is, a student does not know whose homework they are correcting for, and therefore, this will reduce the intention for students to cheat in grading. In addition, the smart contract is designed to make the exchanging order of students randomly. So, even if a student shares their address with friends, there is no guarantee that they will be assigned to do homework correction for each other, especially when many students are enrolled in the course.

The proposed smart contract requires four essential functions to work: (1) submit ciphertext, (2) start the correction, (3) submit plaintext, and (4) fetch the homework

Table 1 Statuses of all functions when function (2) is called

Functions	(1)	(2)	(3)	(4)
After (2) is called	Disabled	Disabled	Enabled	Enabled

that the student needs to correct. As shown in Table 1, initially, only function (1) is activated for students to submit their ciphertext (with commitment). Functions (3) and (4) remain disabled until the teacher calls function (2) when the deadline of the assignment is reached, and the teacher uploads the solutions for grading. At this time, function (1) is also disabled to prevent students from submitting new commitments.

5.2 *Contract for Autonomous Correction and Grading*

Another way to make grading fair to every student is to let the smart contract correct the submissions by itself. This smart contract also has four essential functions, and the first three of them are the same as that of V-A. The fourth one is now changed to function (4) fetch grading results. On calling function (2), the teacher receives the answers and changes the other functions' statuses, as shown in Table 1. The smart contract then corrects and grades a student's answer once the student calls function (3) and uploads the plaintext, which is matched with the verified ciphertext, uploaded by function (1). Finally, function (4) is designed to allow all enrolled students to see their grading results.

Comparing with Sect. 5.1, this approach simplifies students' workloads. It guarantees fairness to all students since the smart contract autonomously corrects every submission by comparing them to the solutions given by the teacher. However, to make this method workable, both the solutions of assignments and their forms in the plaintext domain must be fixed to ensure that the smart contract can match or extract correct solutions from the plaintexts. For this reason, the teacher has to upload their fixed solutions rather than rough guidelines to the assignments. Thus, grading a multiple-opinion essay question is hard to achieve in this case. In other words, this approach requires both students and teachers to be more devoted to do the assignment and upload the solutions, but it does help complete the most exhausting job for everyone and brings true fairness to the grading system.

5.3 *Contract for Supporting Collective Correction*

Our next goal is to make the grading of open-ended questions more convincing by letting the answer of each student be judged on the basis of different opinions. In contrast, it is a general belief that a ridiculous answer to some judge may be a quite

Table 2 Statuses of all functions when function (2) is called (en = enabled/dis = disabled)

Functions	(1)	(2)	(3)	(4)	(5)	(6)	(7)
Deployment	Enable	Enable	Disable	Enable	Disable	Disable	Disable
After (2) is called	Disable	Disable	Enable	Enable	Enable	Enable	Enable

make sense response or even exactly match the point to other judges. Thus, this contract is designated to implement a collective grading framework with the same concept as addressed in Sect. 4.3.

This smart contract consists of seven essential functions: (1) submit ciphertext, (2) start the correction, (3) submit plaintext, (4) register judge, (5) get homework, (6) grade, and (7) get the result. Once again, students need to upload their ciphertexts by function (1) as the commitments, submit the homework answer's plaintext by calling function (3), and after the deadline or after the teacher starts the correction process applying function (2). Notice that function (2) plays only the role of locking and unlock functions, as listed in Table 2, without asking for standard grading procedures to ensure judges follow their own opinions. Function (4) allows the teacher (contract owner) to add judges into the smart contract at any moment, and the judges can then apply function (5) to see every student's information (ciphertext, plaintext, and address) they need for grading the submissions. The judges can upload their grading results by function (6), and the students and the teacher can find the grading results by function (7). The grading results of each student include each score to the student given by different judges and a weighted final score. This smart contract provides an efficient way for collective grading; it helps manage tasks and integrate information into a straightforward platform while ensuring all judges' and students' privacy. Each judgment can be made without referencing others' opinions. With this smart contract, scores are given trustworthily and faithfully so that the final grades reflect a much higher correlation to students' learning outcomes. Thus, the certificate of the course or the achievements accomplished in the course can be more convincing. Finally, for ease of referencing, we list all the pseudocodes of the involved smart contracts in the appendix.

6 Experimental Results

6.1 System Implementation

The proposed work is realized based on the Ethereum architecture with designed application tools for integrating all the mechanisms introduced in Sect. 4. The proposed blockchain system is built based on the Ethereum source code, available in [20], programmed in Go language for simplicity and reproducibility. The application tools are essential keys to make the realized homework grading system much more user friendly. They cover all complex procedures for the users (students and teachers) so that everyone can use the system with ease by few simple selections without understanding the principles and theories of blockchain beforehand, which is a demanded scenario in actual usage.

The application tools include three main modules: the cryptography module, the blockchain module, and the student identity module. Two versions of the application tools are designed for students and teachers; both are built on three programming languages to ensure every function is working properly and stable. That is, Node.js for blockchain interactions, Go for Chaotic Cryptography [25], and Python for user interface, RSA [22] and Secret Sharing [26].

6.2 Randomness of the Chaotic Random Number

In our work, a chaotic-map-based random number generating module is applied to hash the inputted plaintexts to protect students' privacy. Thus, the security of the Chaotic Cryptography module is directly correlated to the randomness of the generated random numbers. This section shows the high randomness of the generated random numbers by observing their distributions and comparing the randomness between two generated results with two seeds differed in a tiny difference. Figure 9 (left) shows the 512 × 512 noise image corresponding to the generated random numbers, with the given seed 12345678, and the associated histogram (c.f. Fig. 9 [right]) verifies that their corresponding distribution is very close to the uniform one. Figure 10 (left) shows another 512 × 512 noise image created with the seed value of 12345677, and as shown in Fig. 10 (right), the resultant histogram is once again very close to the uniform distribution. Although there is only a single-digit difference between the two seeds, the comparison given in Fig. 11 shows there are a tremendous amount of pixel changes (approximately 99.6%) that occurred in the two images. Therefore, the outcomes of the adopted

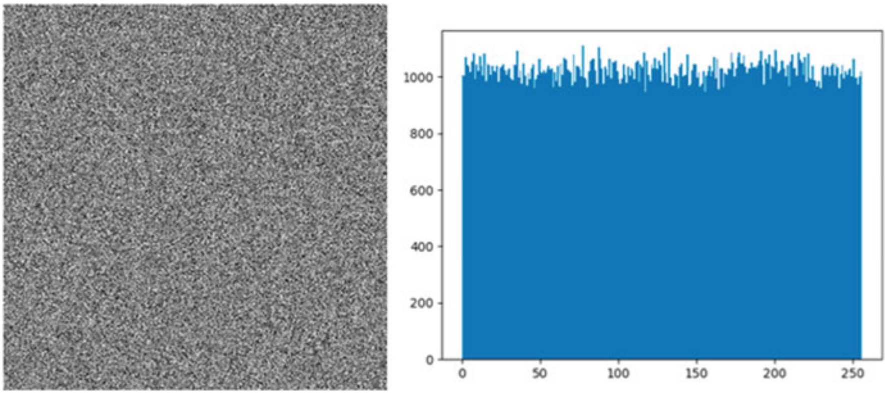


Fig. 9 The noisy image generated with the seed value 12345678

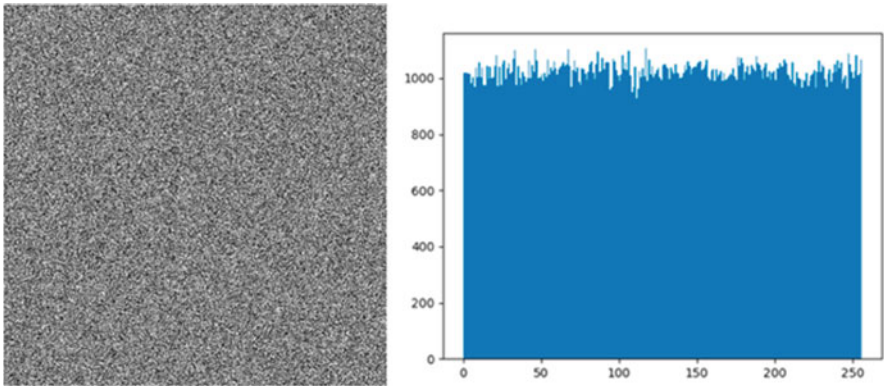
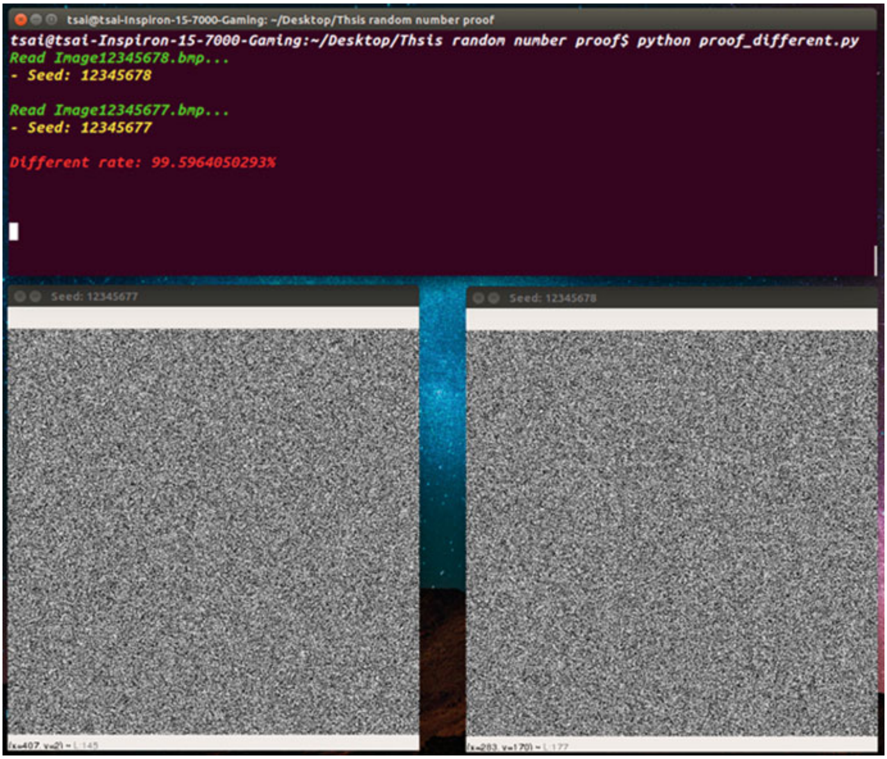


Fig. 10 The noisy image generated with the seed value 12345677


tsai@tsai-Inspiron-15-7000-Gaming: ~/Desktop/Thsis random number proof
Seed: 12345677
Seed: 12345678
(x=407, y=2) ~ L:145
(x=283, y=170) ~ L:177

```
tsai@tsai-Inspiron-15-7000-Gaming:~/Desktop/Thsis random number proof$ python proof_different.py
Read Image12345678.bmp...
- Seed: 12345678

Read Image12345677.bmp...
- Seed: 12345677

Different rate: 99.5964050293%
```

Fig. 11 The two related difference images between the two noisy images given in Figs. 9 and 10

chaotic random number generating module are highly unpredictable and will bring significant benefits to students' privacy security.

6.3 Comparison with Related Work

Comparing our work with the popular online course platform [4] used in our university, a centralized system called CEIBA, our work gets better advantages in system transparency and fairness to students (c.f. Table 3). In a centralized platform, information can be uploaded or deleted without being recorded; those actions cannot be tracked by involved members (mostly students); thus, students or teachers may miss some deleted information and often result in dissensions. Additionally, if students directly use their identities to interact with their teachers, this may allow teachers to treat each student differently, more or less. Therefore, using blockchain properties to track every information and activity openly will make the system much more transparent to avoid unnecessary disputes between students and teachers by treating every on-chain member equally. Those smart contracts introduced in Sect. 5 help teachers distribute some heavy works and ensure better fairness to every student. Moreover, the cryptosystem used in this work can prevent students from cheating and encourage them to learn with the right attitudes. The proposed work can also perform with higher stability, longer liveness, and better data preservation because all the members, including students, teachers, and the system administrator, are willing to maintain the system's operations. In contrast, in the traditional platforms, only the administrator is devoted to system maintenance.

Since many cryptographic algorithms are used in this work, the time spent uploading homework or announcements is usually higher than that of a traditional platform. For example, uploading a homework answer to a conventional online course platform takes just about a few seconds; however, in the proposed work, students have to encrypt their homework answers before uploading them. In other words, it may take one or two or more minutes, depending on the size of the uploaded hand-in answers.

Table 3 Comparison of the proposed work and the traditional online course platform, CEIBA

	The proposed work	Traditional educational online Platform (CEIBA)
Decentralized	Decentralized	Centralized
Transparency	Blockchain property	Centralized
Fairness	Smart contract, blockchain property	Depend on teachers
Prevent cheating	Cryptography, blockchain property	–
Speed	Latency due to encryption/decryption	–
Data preservation	Maintained by all members	Centralized
Liveness, stability	Depend on all members	Depend on administrator

7 Discussion and Conclusion

The design of the proposed system focuses mainly on the realization of a transparent and fair homework correction and grading platform based on blockchain technology. Although it is expected to establish an efficient way for supervising grading-related activities and ensuring fairness to all members, the latency caused by the involved encryption processes becomes the major obstacle to its usage in practice. The most apparent latency is caused by the RSA module, which takes approximately 1 min to encrypt plaintext with just 100 words. Fortunately, this comes from the considerable time cost of loop expressions in Python, and it can be much speeded up when appropriate language, such as C++, is used instead.

The "Grading by Exchanging" smart contract works relying on the submission order of students' hand-in homework answers. There was a possible vulnerability when a group of students conspired to upload their homework assignments (in ciphertext form) simultaneously. Under this situation, they will have a higher chance of cheating on each other. Using hash functions to generate random numbers can indeed make the exchanging behavior even more unpredictable. Still, again, this may result in too many costs for calculation (e.g., gases in Ethereum blockchain) when too many students are enrolled in the course. On the other hand, the random numbers are predictable by those who decide the seeds of the hash functions (e.g., the responsible teachers) or those who generate the blocks (i.e., the miners).

Finally, the properties claimed in this work have been tested and proved stable with 10–20 nodes run on the same personal computer. The stability of the involved blockchain is expected to handle lots of users since it is Ethereum based reliably. Of course, a real public test of the system is a must before it is ready to be deployed in practical usage.

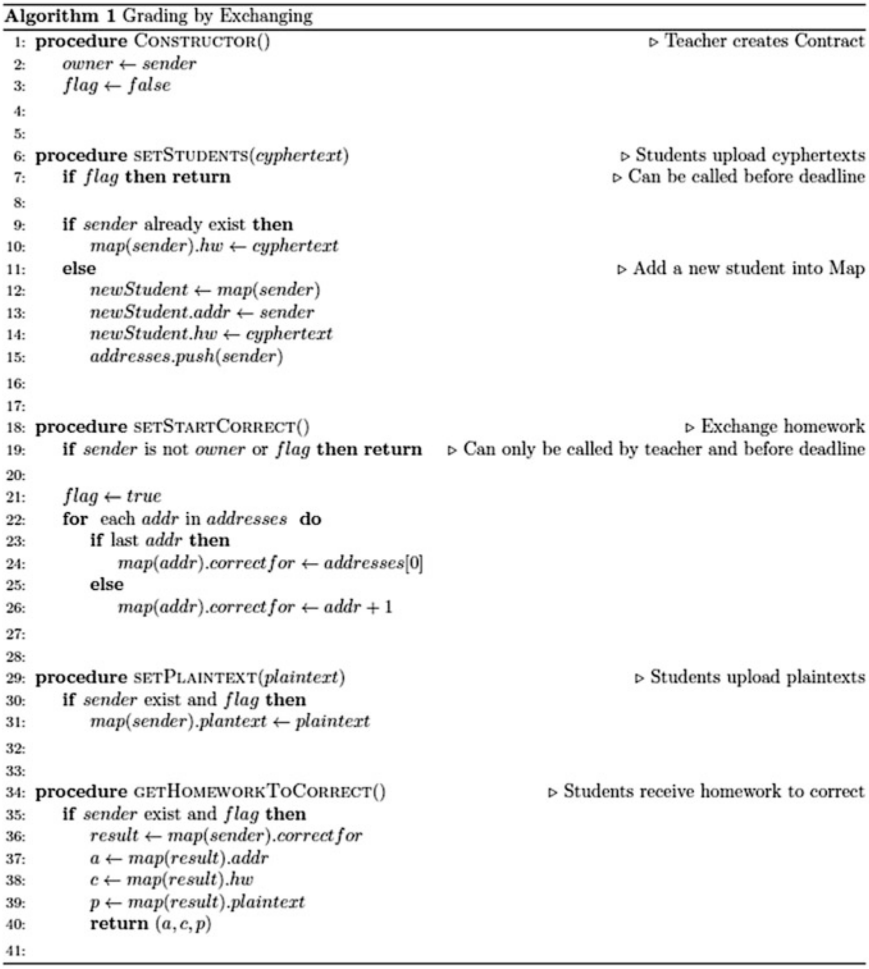
To increase the practical value of our current system, the user interface should be designed friendlier; for example, realizing the function selection based on keystrokes, which is more intuitive to most people. Some procedures in our design can be done automatically, such as decrypting ciphertext once the teacher's account has received a certain amount of hand-in homework from students. Other works for improving our system's practicability include: supporting various types of files (PDF, images, etc.), allowing users to choose their files instead of asking them to transfer their messages into specific file formats, and helping users back up their passwords to recover them whenever necessary, etc.

As for the involved cryptographic techniques, many algorithms claimed to have better performances in timing and security; therefore, applying those methods to upgrade our system is worthy of doing. For example, to achieve natural fairness to all members, picking another random number generator with higher randomness and efficiency (i.e., it will introduce less computational cost) on the Solidity is an essential task for contract design to provide more unpredictability.

Of course, in the future, combining our work with other related works to integrate the merits of blockchain technology into higher-level education usages, such as sharing and maintaining students' certificates and learning results between institutions and colleges, is of great interest. Nevertheless, this goal is currently difficult to achieve since it requires the support of cross-chain techniques which allow the interactions between different blockchains. This direction is worthy of devoting because we can build a complete blockchain-based educational system based on the above cross-chain system integration. We can then achieve information sharing between institutions and conduct fundamental interactions between teachers and students to establish an actual transparent and fair education system for all students, teachers, and administration staff.

Appendix

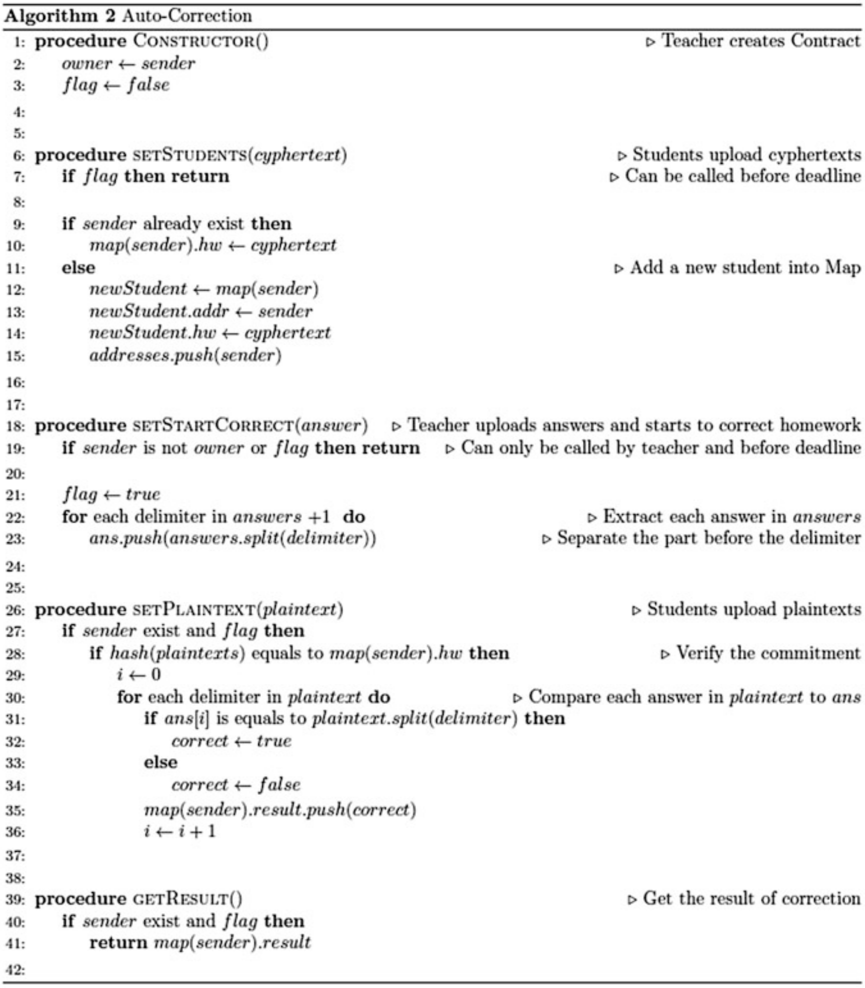
A.1. Pseudocodes of the "Grading by Exchanging" Smart Contract



Algorithm 1 Grading by Exchanging

```
procedure CONSTRUCTOR()                                   ▷ Teacher creates Contract
    $owner \leftarrow sender$
    $flag \leftarrow false$


procedure SETSTUDENTS($cyphertext$)                        ▷ Students upload cyphertexts
    if $flag$ then return                                  ▷ Can be called before deadline

    if $sender$ already exist then
        $map(sender).hw \leftarrow cyphertext$
    else                                                   ▷ Add a new student into Map
        $newStudent \leftarrow map(sender)$
        $newStudent.addr \leftarrow sender$
        $newStudent.hw \leftarrow cyphertext$
        $addresses.push(sender)$


procedure SETSTARTCORRECT()                                ▷ Exchange homework
    if $sender$ is not $owner$ or $flag$ then return   ▷ Can only be called by teacher and before deadline

    $flag \leftarrow true$
    for each $addr$ in $addresses$ do
        if last $addr$ then
            $map(addr).correctfor \leftarrow addresses[0]$
        else
            $map(addr).correctfor \leftarrow addr + 1$


procedure SETPLAINTEXT($plaintext$)                        ▷ Students upload plaintexts
    if $sender$ exist and $flag$ then
        $map(sender).plantext \leftarrow plaintext$


procedure GETHOMEWORKTOCORRECT()                           ▷ Students receive homework to correct
    if $sender$ exist and $flag$ then
        $result \leftarrow map(sender).correctfor$
        $a \leftarrow map(result).addr$
        $c \leftarrow map(result).hw$
        $p \leftarrow map(result).plaintext$
        return $(a, c, p)$
```

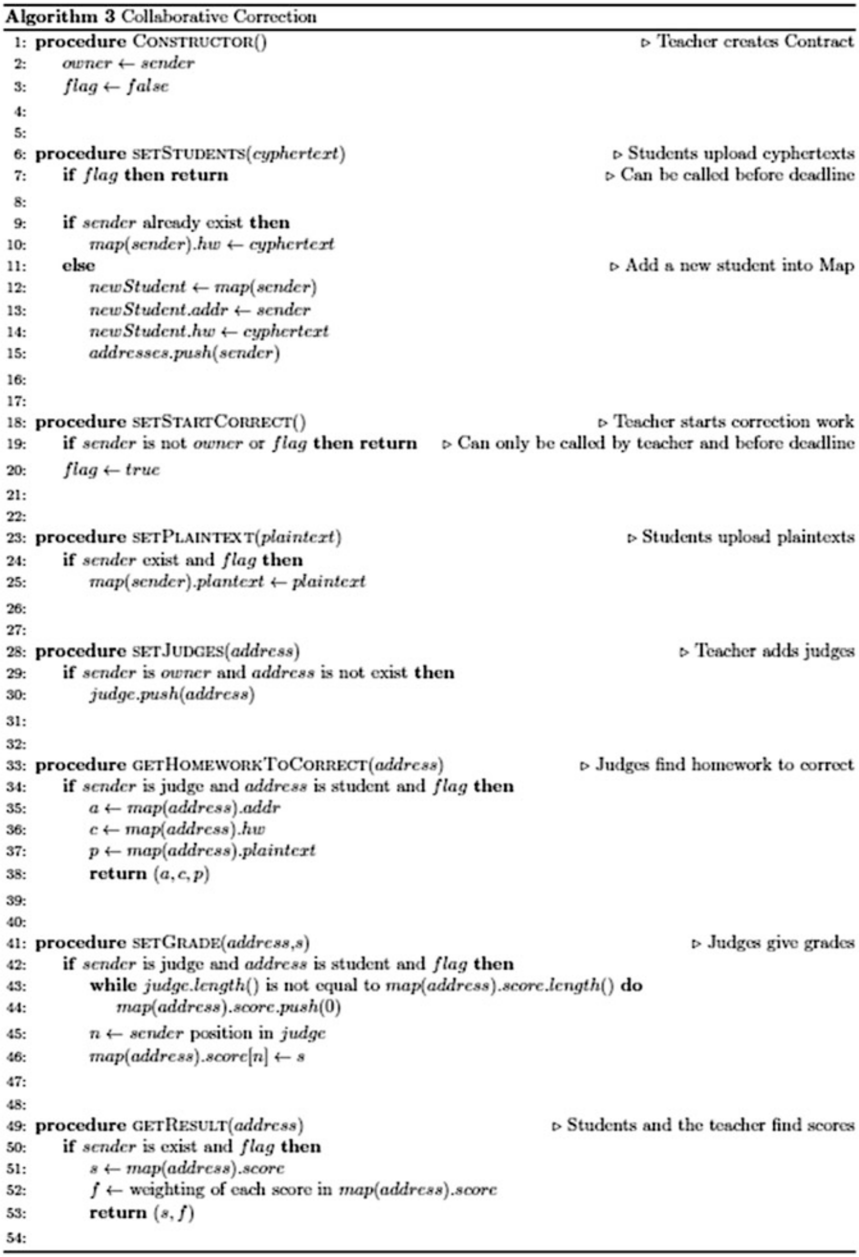
A.2. Pseudocodes of the "Auto-correction" Smart Contract



Algorithm 2 Auto-Correction

```
procedure CONSTRUCTOR()                                   ▷ Teacher creates Contract
    owner ← sender
    flag ← false


procedure SETSTUDENTS(cyphertext)                         ▷ Students upload cyphertexts
    if flag then return                                   ▷ Can be called before deadline

    if sender already exist then
        map(sender).hw ← cyphertext
    else                                                  ▷ Add a new student into Map
        newStudent ← map(sender)
        newStudent.addr ← sender
        newStudent.hw ← cyphertext
        addresses.push(sender)


procedure SETSTARTCORRECT(answer)    ▷ Teacher uploads answers and starts to correct homework
    if sender is not owner or flag then return    ▷ Can only be called by teacher and before deadline

    flag ← true
    for each delimiter in answers +1 do                   ▷ Extract each answer in answers
        ans.push(answers.split(delimiter))                ▷ Separate the part before the delimiter


procedure SETPLAINTEXT(plaintext)                         ▷ Students upload plaintexts
    if sender exist and flag then
        if hash(plaintexts) equals to map(sender).hw then ▷ Verify the commitment
            i ← 0
            for each delimiter in plaintext do            ▷ Compare each answer in plaintext to ans
                if ans[i] is equals to plaintext.split(delimiter) then
                    correct ← true
                else
                    correct ← false
                map(sender).result.push(correct)
                i ← i + 1


procedure GETRESULT()                                     ▷ Get the result of correction
    if sender exist and flag then
        return map(sender).result

```

A.3. Pseudocodes of the “Collective Correction” Smart Contract



Algorithm 3 Collaborative Correction

```
procedure CONSTRUCTOR()                                        ▷ Teacher creates Contract
    $owner \leftarrow sender$
    $flag \leftarrow false$


procedure SETSTUDENTS($cyphertext$)                            ▷ Students upload cyphertexts
    if $flag$ then return                                      ▷ Can be called before deadline

    if $sender$ already exist then
        $map(sender).hw \leftarrow cyphertext$
    else                                                       ▷ Add a new student into Map
        $newStudent \leftarrow map(sender)$
        $newStudent.addr \leftarrow sender$
        $newStudent.hw \leftarrow cyphertext$
        $addresses.push(sender)$


procedure SETSTARTCORRECT()                                    ▷ Teacher starts correction work
    if $sender$ is not $owner$ or $flag$ then return    ▷ Can only be called by teacher and before deadline
    $flag \leftarrow true$


procedure SETPLAINTEXT($plaintext$)                            ▷ Students upload plaintexts
    if $sender$ exist and $flag$ then
        $map(sender).plantext \leftarrow plaintext$


procedure SETJUDGES($address$)                                 ▷ Teacher adds judges
    if $sender$ is $owner$ and $address$ is not exist then
        $judge.push(address)$


procedure GETHOMEWORKTOCORRECT($address$)                      ▷ Judges find homework to correct
    if $sender$ is judge and $address$ is student and $flag$ then
        $a \leftarrow map(address).addr$
        $c \leftarrow map(address).hw$
        $p \leftarrow map(address).plaintext$
        return $(a, c, p)$


procedure SETGRADE($address$,$s$)                              ▷ Judges give grades
    if $sender$ is judge and $address$ is student and $flag$ then
        while $judge.length()$ is not equal to $map(address).score.length()$ do
            $map(address).score.push(0)$
        $n \leftarrow sender$ position in $judge$
        $map(address).score[n] \leftarrow s$


procedure GETRESULT($address$)                                 ▷ Students and the teacher find scores
    if $sender$ is exist and $flag$ then
        $s \leftarrow map(address).score$
        $f \leftarrow$ weighting of each score in $map(address).score$
        return $(s, f)$

```

References

1. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Solidity — Solidity 0.4.25 documentation (2008), https://solidity.readthedocs.io/en/v0.4.25/
2. Massive open online course, https://en.wikipedia.org/wiki/Massive_open_online_course
3. Welcome to MOOC.org, https://www.mooc.org/#mooc-topics
4. NTU Ceiba, https://ceiba.ntu.edu.tw/
5. H. Sun, X. Wang, X. Wang, Application of blockchain technology in online education. Int. J. Emerging Technol. Learn. (iJET) **13**(10), 252–259 (2018)
6. S.S. Smith, Blockchain and online learning are a powerful combination. Forbes, https://www.forbes.com/sites/seansteinsmith/2020/08/31/blockchain-and-online-learning-are-a-powerful-combination/?sh=6a4d73d718d3
7. Power of work, https://en.wikipedia.org/wiki/Proof_of_work
8. V.K. Das, Role of directed acyclic graphs in the blockchain landscape, https://www.blockchain-council.org/blockchain/role-of-directed-acyclic-graphs-in-the-blockchain-landscape/
9. Elliptic-curve cryptography, https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
10. R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978). https://doi.org/10.1145/359340.359342
11. R.C. Merkle, A digital signature based on a conventional encryption function, advances in cryptology, CRYPTO '87. Lect. Notes Comput. Sci. **293**, 369. ISBN 978-3-540-18796-7 (1988). https://doi.org/10.1007/3-540-48184-2_32
12. G. Chen, B. Xu, M. Lu, N.-S. Chen, Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. **5**(1), 1–10 (2018). https://doi.org/10.1186/s40561-017-0050-x
13. D.J. Skiba, The potential of Blockchain in education and health care. Nurse Educ. Perspect. **38**(4), 220–221 (2017). https://doi.org/10.1097/01.NEP.0000000000000190
14. P. Edastama, N. Lutfiani, Q. Aini, S. Purnama, I.Y. Annisa, Blockchain encryption on student academic transcripts using a smart contract. J. Educ. Sci. Technol. (EST) **7**(2), 126–133 (2021)
15. S.A. Mansoori, P. Maheshwari, A framework to implement blockchain in higher education institutions, in *International Conference on Emerging Technologies and Intelligent Systems*, (Springer, Cham, 2021, June), pp. 244–254
16. M. Sharples, J. Domingue, The blockchain and kudos: A distributed system for educational record, reputation and reward, in *European Conference on Technology Enhanced Learning*, (Springer, Cham, 2016), pp. 490–496. https://doi.org/10.1007/978-3-319-45153-4_48
17. M. Turkanovic, M. Hölbl, K. Kosic, M. Herciko, A. Kamisalic, EduCTX: A blockchain-based higher education credit platform. IEEE Access **6**, 5112–5127 (2018). https://doi.org/10.1109/ACCESS.2018.2789929
18. M.B. Hoy, An introduction to the Blockchain and its implications for libraries and medicine. Med. Ref. Serv. Q. **36**(3), 273–279 (2017). https://doi.org/10.1080/02763869.2017.1332261
19. Ethereum, https://en.wikipedia.org/wiki/Ethereum
20. Source code of go-ethereum, https://github.com/ethereum/go-ethereum
21. Solidity — solidity 0.4.25 documentation, https://solidity.readthedocs.io/en/v0.4.25/
22. RSA implementation in Python, https://github.com/jchen2186/rsa-implementation, 2017
23. A. Shamir, How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
24. L. Kocarev, Chaos-based cryptography: A brief overview. IEEE Circuits Syst. Mag. **1**(3), 7–21 (2002). https://doi.org/10.1109/7384.963463
25. A. Briese, Work draft 'breeze – A chaos based pseudo random number generator by hopping between logistic map pseudo orbits' (2014), https://github.com/AndreasBriese/breeze
26. R. Shea, M. Ali, M. Flaxman, Secret-sharing (2015), https://github.com/blockstack/secret-sharing

Improving Supply Chain Management Performance with Blockchain Technology

Saurav Negi

1 Introduction

Blockchain has become one of today's most popular buzzwords, and its applications and operations have flourished in recent years. This technology is now seen to have the ability to transform not only the financial sector but a variety of other industries due to its ability to be used without the involvement of intermediaries or central authorities [83]. Due to its ability to validate double-spend payments, it was first used in the finance sector [32]. However, blockchain technology (BT) has expanded beyond finance in recent years, demonstrating its utility as an underlying technology in several industries, comprising power, tourism, and, most notably, supply chain management (SCM) [81].

A supply chain (SC) is defined as "the set of organizations and connections that cumulatively define the materials and information flow both downstream toward the customer and upstream toward the very first supplier," according to Schroeder et al. [85, p. 223]. Technology can be utilized to promote communication and transparency between SC participants in SCM [37].

Modern SCs have seen significant transformations recently, transforming a formerly operational activity into a stand-alone SCM function [4]. Many logistical operations are included in SC processes, such as "planning, implementing, and managing the efficient flow and storage of goods, services, and related information from the source to the point of consumption to meet consumer needs" [20]. Streamlining and integrating these tasks provides a competitive edge concerning revenue optimization, transparency, high inventory turnover, efficient customer service, and SC speed [82]. However, achieving these goals is difficult because of

S. Negi (✉)
Modern College of Business and Science (MCBS), Muscat, Oman
e-mail: Saurav.Negi@mcbs.edu.om

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_14

the higher complexities in the SC due to the interaction of various geographically diverse organizations acting independently and regularly competing to provide better customer services [12, 63, 84, 99]. Apart from complexities, SCs face a variety of uncertainties and risks [17, 18, 39, 95], including trading members engaged in opportunistic actions (e.g., cheating, distorting information) [51], privacy leakage [111], fraud and cybercrime [10], and fake product recognition [81]. Managing information in the SC is difficult because reliability and real time are required to prevent any risks, fraud, and poor performance [84, 91]. A better verification and information sharing system is needed to enhance the reliability, authenticity, and traceability of data [45, 84].

Due to the complexity of processes, the number of documents, and global collaborations, the SC is regarded as a vital sector of the business and is recognized by various experts as the one with the highest potential for the adoption of management-assist technologies [51]. Under the influence of the fourth industrial revolution, businesses began leveraging technology to streamline processes and save costs to boost their local and global competitiveness. Following the introduction of integrated systems, tools such as radio-frequency identification (RFID), big data, and the Internet of Things (IoT) have been used to focus on trying to minimize bottlenecks and facilitate managers in making decisions based on data generated by their operations through predictive analytics [5].

Corporate leaders in a variety of industries are attempting to improve SCM through digitalization to address SC challenges [53]. The digitalization of SCs refers to the "process of businesses adopting inter-organizational systems to interact and transact with their trading partners (e.g., important suppliers and customers) along with their respective SCs" [81]. In the digitalization era, BT is regarded as one of the most important SCM tools [78]. It is a distributed ledger that employs cryptography to process data ("smart contracts") and add it to a data chain, making the process transparent from beginning to end [69]. Inventory management, product traceability and origin, logistics, process analysis, risk reduction, and sustainability are just a few of the areas where blockchain may help decision-makers [19, 51, 84, 98].

Blockchain-enabled SCs are becoming more common and are proving to be quite effective. "Depending on the product, the SC can span over hundreds of stages, multiple geographical (international) locations, a multitude of invoices and payments, have several individuals and entities involved, and extend over months. Due to the complexity and lack of transparency of our current SCs, there is interest in how blockchains might transform the SC and logistics industry" [64]. The technology's earliest and most well-known application is Bitcoin [69], "a peer-to-peer digital cash system that enables parties to make payments without any financial institution acting as a trusted third-party intermediary" [21]. Electronic money, such as Bitcoin, has gained popularity in recent years because of improved usage in both offline and online markets, as well as the significant variation in the value of money in the e-money transactions market. The BT underpins this digital currency [4, 20]. BT offers benefits like greater transparency, immutability, and "smart contracts" to enhance connectivity and reliability, both of which are necessary for SC collaboration [82].

Blockchain has drawn the interest of various academicians and professionals from numerous sectors because it has the potential to improve data security, data immutability, trust, transparency, and traceability in the SC [32, 112]. By 2025, global investment in BT is estimated to reach USD 176 billion [50].

The primary features of blockchain, such as decentralization, intangibility, and transparency [93], have augmented the interest of researchers, entrepreneurs, and governments interested in learning more about the benefits that this technology can provide to a variety of industries [45]. Blockchain applications are not limited to the finance business. They are already being used in a variety of industries. For example, BT is being discussed in a range of industries, involving healthcare [27, 51, 90], tourism [30, 73, 74, 100], social media and marketing [17, 18, 80], finance [86], e-commerce [58, 101], energy [110], education [35], agriculture [61], transportation [71], and humanitarian action [8, 9, 24, 25, 75, 113].

Similarly, blockchain research has gained plenty of attention, especially from the logistics and SCM sectors [2, 3, 23, 32, 46, 106, 108].

As a result, this chapter aims to illustrate how BT may be utilized to improve SCM and overall business performance. To answer the following research questions, the study employed a systematic review approach:

- What are the applications of BT to improve an organization's SC performance?
- What are the benefits and challenges of incorporating BT into the SC?

The present study contributes to the SCM literature by describing the contributions of BT to SC performance based on blockchain properties like traceability, transparency, security, and real-time data exchange. Both practitioners and academics may find the study useful as a starting point for additional debate and research. The research also makes recommendations for future research on BT in SCs.

The remainder of the chapter is structured as follows. The methodology is presented in Sect. 2. Section 3 explains the BT and describes the functioning of the BT. Section 4 presented the application of BT in SC, as well as the use of BT to improve SC performance. The benefits and challenges of BT in SCM are discussed in Sect. 5. The study's conclusion is offered in Sect. 6, including the study's contributions and constraints, as well as a research agenda to direct future research.

2 Methodology

This chapter examines BT and its possible applications in SCM to help businesses improve their performance. This chapter serves as guidelines for possible use within the SC community, as well as to propose future study and exploration areas. The study analyzed available literature to determine the application of BT in SCM and its associated benefits and challenges. This study identifies the primary articles on the subject that are available in academic databases (primarily in Scopus as it offers more coverage than WoS and any other database [[29]]) using the following keywords "blockchain," "blockchain technology," "blockchain in the supply chain," etc. Then, the studies were screened, and the only studies that served the purpose were included for review. The collected studies were then analyzed to understand BT and its role in the supply chain. Based on that, the author presented the narrative review to explain the concept of BT, its applications, benefits, and associated challenges. The studies which were referred to write this chapter range mainly from 2015 to 2021, as most of the studies related to blockchain are carried out during this period. The secondary data was collected from the research papers, reports, chapters, and proceedings. Some of the highly reputed journals that are referred to for this study are *Supply Chain Management: An International Journal*; *International Journal of Production Research*; *Sustainability*; *Supply Chain Forum: An International Journal*; *International Journal of Logistics Management*; *Journal of Operations Management*; *International Journal of Production Economics*; *International Journal of Physical Distribution & Logistics Management*; *Frontiers in Blockchain*; *Electronic Commerce Research and Applications*; *IEEE Transactions on Engineering Management*; *IEEE Transactions on Systems, Man, and Cybernetics: Systems*; *Computers & Industrial Engineering*; *International Journal of Information Management*; *Information Processing and Management*; and *Manufacturing and Service Operations Management.*

3 Overview of Blockchain Technology

Satoshi Nakamoto was the first to conceptualize and introduce BT in 2008 [69]. L'Hermitte and Nair [55] define blockchain as a "distributed ledger system or a shared data platform that enables authorized communication and widespread sharing of real-time information among participants." It's a distributed data structure where the data is exchanged between peers through a network. A blockchain is made up of a chain of blocks that documents/track transactions between participants. Transactions in a peer-to-peer network must be approved and confirmed by the members in a network according to an established protocol. The transaction data are maintained on a distributed ledger, which is a public ledger [34]. A "distributed ledger" records transactions in a decentralized manner. All network users have access to the same blocks, which can be viewed by anyone. When specific members of the network originate and validate a transaction/block, it is connected to prior blocks by adding to the network [33, 104]. Individuals, robots, algorithms, and organizations can all execute transaction verification. Blockchain is viewed as an alternate tool for forming networks, not just among individuals but also among businesses [54]. Blockchain can cut out middlemen in a network and connect participants directly, potentially lowering transaction costs and human error. Storing data in shared databases rather than centralized ones decreases the data loss risk and improves security and information transparency [28].

"Smart contracts" are digital agreements that can be created using BT. According to Crosby et al. [21], "A smart contract is a computer code embedded in the blockchain. It establishes a set of pre-determined conditions agreed upon by the participants, verifies the performance of the parties, and automatically executes the terms of the agreement as soon as pre-programmed conditions are met. 'Smart contracts' are, therefore, enforced by computer protocols, without any human intervention and manual paperwork." "Smart contracts" lower transaction costs by eliminating the need for intermediates [57]. "Smart contracts" improve information privacy and security since all transactions must adhere to the inherent legal agreements and must be accepted and confirmed by the participants based on the "smart contracts" transaction validation standards [28, 91].

Blockchain has the ability to fundamentally alter the way a wide variety of companies operate [72]. Blockchain, according to IBM [42], can benefit businesses in a variety of industries by speeding up operations, freeing up money, lowering transaction costs, and ensuring trust and security. BT has sparked a lot of interest all over the world and in a variety of industries. The United States' "Defense Advanced Research Projects Agency" (DARPA) is looking into using blockchain for a messaging service. The United Kingdom, Russia, Estonia, and Delaware in the United States have investigated blockchain applications for commercial vendors, public record-keeping, and voting systems. Banks have already organized consortiums and research labs focusing on the blockchain applications possibilities in the financial sector [48].

Blockchain is rapidly transforming the digital tools used to operate daily transactions [113], and a plethora of studies show that blockchain's innovative and diversified qualities present several potential in a variety of application sectors. Furthermore, it does not require the involvement of a third party, reducing transaction costs and charges [83].

3.1 Functioning of Blockchain Technology

The blockchain, as depicted in Fig. 1, is a "chain of blocks" that compiles a sequence of transactions carried out within a process, therefore the name "blockchain." In a word, a blockchain is a database that consists of a continuously growing series of timestamped blocks holding data [102].

According to Piscini et al. [76], "blockchain is assuming the role of trusted gatekeeper and purveyor of transparency." It allows for the secure and efficient transfer of resources among parties who do not know or trust one another. First, blockchain's ability to store and disseminate relevant data like transaction logs, security records, and histories builds trust and transparency. In turn, this provides network participants with more influence over exchange operations [76]. Second, blockchain creates a trail of safe, unchangeable, and shareable transaction records that can be traced back to network participants via a cryptographic signature

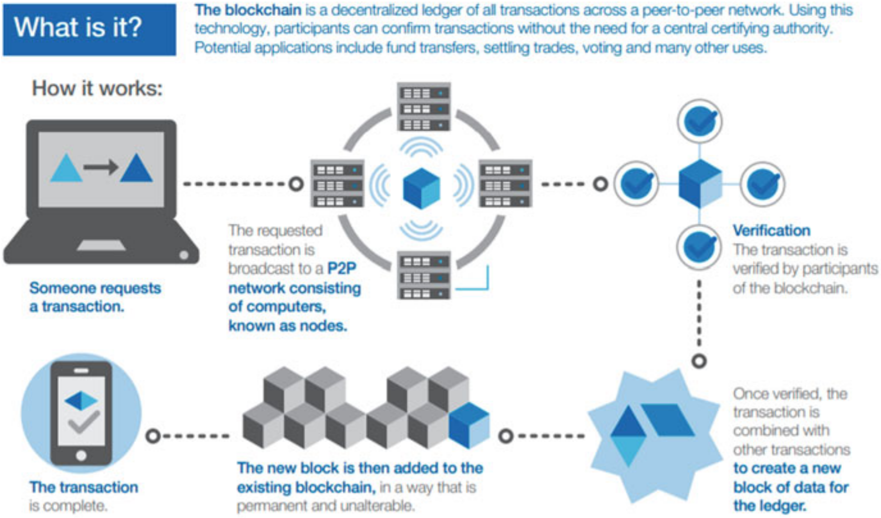

What is it?
The blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Using this technology, participants can confirm transactions without the need for a central certifying authority. Potential applications include fund transfers, settling trades, voting and many other uses.
How it works:
Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Verification
The transaction is verified by participants of the blockchain.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Fig. 1 A look at blockchain technology. (Source: World Economic Forum [109])

method. Third, trust is generated via technology's ability to create unchangeable consensus-based norms. These terms and conditions are stored in the "smart contract" codes and the system's algorithms. Lastly, trust is built based on self-executing contracts (autonomous contract execution) and automated monitoring of the members' adherence to the conditions. Pre-agreed transactions occur automatically upon fulfillment of the contract's conditions, with no hassle or risk of mistake [11, 40, 76].

3.2 *When Does Blockchain Make Sense?*

Blockchain technology, like any new technology, has its own set of benefits and drawbacks. Practitioners must decide whether BT is the best tool for a specific issue or topic or whether another tool would be more appropriate.

Blockchain technologies are more valuable:

- When there is no central authority in place that is well established and effective
- When it is desirable to have a record or verification of transactions
- When there are several parties or actors involved
- When they are used to track ownership of complicated things over time
- When the groups or actors are engaged must work together

4 Application of Blockchain Technology in Supply Chain Management

Several authors suggested using blockchain in various SCs for automation, smart contracting, tracking, tracing, data management, and other purposes [23, 38, 70, 88].

There are four primary properties of blockchains that make them appealing in the context of SCM. First, because the blockchain is meant to be distributed and synchronized across networks, it encourages data contribution from all parties involved, making it ideal for multiorganizational trade systems such as SCs. Second, the blockchain is constructed on peer-to-peer networks, which need unanimous agreement from all appropriate groups that a transaction is legitimate, preventing erroneous or potentially fraudulent transactions from being stored in the database. Third, the data's immutability ensures that agreed-upon operations are recorded and unchanged. This ensures asset source, which implies that it is feasible to establish the location of an asset, its history, and the events that occurred throughout its life [6, 19]. Fourth, "smart contracts" are supported by some blockchains. Contrary to its name, a "smart contract" is not a legally binding agreement, but rather a computer protocol or trusted program that runs on the blockchain's nodes [15]. The objective of a "smart contract" is to digitally enable, verify, or enforce the terms of a contract, enabling trustworthy transactions without any need for third-party involvement. These protocols can be used to assess whether a given action, such as a payment, should be approved. In comparison to standard contracts, "smart contracts" provide the advantages of decreasing risk, cutting service and administrative costs, and boosting the efficiency of business processes [6]. "Smart contracts," moreover, could build trust among parties [7].

Blockchain is seen as a game-changing technology with enormous potential in SC and logistics management. Blockchain is expected to radically change SC operations by substantially increasing trust, visibility, transparency, and traceability [55, 77, 103] and resistance when linked with technological advances such as IoT, RFID, and data analytics [66]. Blockchain helps SC organizations to answer questions like "Where is my container?" and "Under what conditions were my products transported?" by breaking down data silos and improving business-to-business connectivity [105]. More specifically, blockchain monitors each transaction (from items ordered through the receiving of the items, the invoice, and the financial settlement), removes paperwork, and, as a result, helps to reduce cost, delays, and errors throughout the SC [97].

According to recent studies, there is significant interest in the application of blockchain in SC and operations management (e.g., [60]). According to Queiroz et al. [79], SC scholars have discovered blockchain contributions such as improving SC efficiency, persuading new product design and development, minimizing the need for intermediaries, advancing inventory management and replenishment, advancing sustainable SCM, reducing illegal counterfeiting, improving quality management, and enhancing product safety and security. According to Queiroz and Wamba [78], “blockchain can improve information flow (document workflow management), financial transactions (data confidentiality), and SC coordination (device connectivity).” According to Wang et al. [106], blockchain allows for more SC integration, which improves overall SC performance. According to Kshetri [51], the blockchain-based SC increases customer confidence by offering benefits such as real-time product tracking, lower product moving costs, extremely secure transactions, and protection against product counterfeiting. According to Kouhizadeh and Sarkis [49], the openness, visibility, and security properties of blockchains foster trust in commercial SCs and can eliminate or at least reveal any hidden unethical behavior by SC participants. In conclusion, the potential of blockchain for SCM is that it will significantly improve visibility, accountability, traceability, and the trustworthiness of relationships [8, 9].

BT has the potential to contribute significantly to SC operations in a wide range of businesses [67, 68], including pharmaceuticals [41], agri-food products, and luxury products, by creating background knowledge and, as a result, decreasing consumer risk perceptions [13, 14, 96]. The properties and advantages of BT, such as real-time information sharing, data security, transparency, and traceability can assist numerous businesses’ SCs [28, 33, 45, 47].

5 Benefits and Challenges in Applying Blockchain Technology in the Supply Chain

This section discusses the benefits of BT application in the SCM and the related challenges.

5.1 Benefits

Due to its ability to track the flow of commodities in real time and improve the visibility and transparency of operations, BT was introduced in this field with the promise of fixing the SC’s key problems [5, 51, 84]. Because all transactions will be authenticated by a group of partners, these benefits can increase transaction security [59, 62] and partner trust [39]. Furthermore, BT can save costs [98] and eliminate hazards associated with product provenance and quality [51, 67, 68]. The following are the benefits that BT provides to improve an organization’s SC performance:

- *Lower transaction costs:* By “connecting people and organizations closely together through a shared ledger and distributed processing over a network,” the blockchain allows actors to transfer value without the use of a middleman [36].

This eliminates many of the costs associated with using a third party to facilitate transactions.

- *Distributed data structure:* The blockchain's main innovation is that it allows actors to interact directly with one another without any requirement for a middleman to oversee exchanges [48]. Blockchain is a distributed data format that connects SC stakeholders via a peer-to-peer network. All parties concur on standardized protocols, which are then used to communicate and validate data [1, 16]. The decentralized structure of blockchain allows for direct transaction verification among parties, eliminating the need for intermediaries [28, 48].
- *Transparency and accountability:* One of the main attributes of blockchain is "transparency," which implies information sharing among SC partners [26]. BT allows stakeholders in the SC network to share real-time information, increasing transparency and reliability among SC partners and customers [32, 84]. The blockchain creates a permanent public ledger. This makes open and transparent data more readily available. It has a favorable impact on SC transaction reliability and trustworthiness, SC operations, SC activity time, and decision-making effectiveness [47, 91].
- *Faster transaction times:* When compared to current financial transaction technologies in the banking system, the blockchain provides a significantly faster way. On a blockchain, "smart contracts" are almost instantaneous [48].
- *Traceability and usage information:* Blockchain facilitates customers to acquire accurate and valid data about items and processes [84, 91]. Another attribute of blockchain is "traceability," which refers to identifying and validating the series of events and components in all stages of a chain. It's critical to keep track of information across the SC to ensure compliance with standards and track down failures [89]. Stakeholders can track and monitor items and shipments along the SC owing to traceability [52, 56]. The traceability feature of blockchain improves the transparency of SC activities, which in turn improves trust among SC stakeholders, such as suppliers and customers, decreases conflicts, lowers verification costs, and allows stakeholders to detect unethical actions [32, 47]. Actors can see the source and timing of each action because the blockchain stores, verifies, and timestamps every action on the network.
- *Encryption of data:* Blockchain allows organizations in the SC network to securely communicate, retrieve, and validate information since data and transactions are cryptographically safeguarded [16]. Advanced cryptography decreases the chance of information loss and alteration, as well as human mistakes in transactions [28, 91]. "Anyone can upload anything to the blockchain, just like they can on the internet, but the reliability and veracity of that material are established by whoever's digital signature was utilized" [31].

The benefits of BT in SC are also summarized in Fig. 2.

In a nutshell, BT improves SC performance by increasing collaboration [25], leveraging relationships with 3PL service providers [7], enhancing traceability

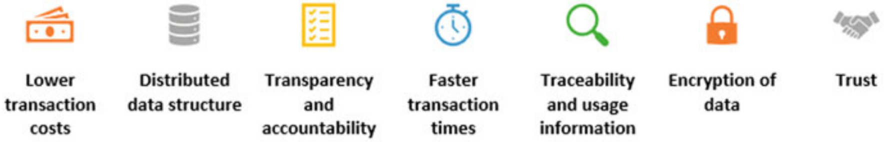

Lower transaction costs
Distributed data structure
Transparency and accountability
Faster transaction times
Traceability and usage information
Encryption of data
Trust

Fig. 2 Benefits of blockchain in SCM. (Source: Author)

and cost-efficiency [43], improving coordination and reducing intermediaries [44], increasing trust [22, 24], and ensuring security, accountability, and transparency [87].

5.2 Challenges

The challenges of BT in a SC can be categorized as the following:

- *New technology:* The technology is still in its early stages. Because present applications are restricted and untested, it's difficult to see their entire potential and repercussions. Furthermore, because the majority of blockchain applications are now vendor driven, more development is required at this early stage [48].
- *Scalability limitations:* As BT is still in its early stages, the technology can only be scaled within its existing applications, as essential algorithms or other advancements have yet to be developed. New advancements, such as BigChainDB [65], have begun to address this issue by creating new algorithms.
- *Internet access and infrastructure:* Using BT necessitates Internet access; places with insufficient capacity or infrastructure are not suitable for blockchain applications. This digital divide also exists in terms of technological knowledge between people who understand how to "operate securely on the Internet" and those who do not [92].
- *Technical challenges in comprehending BT:* BT is new, complex, and difficult to comprehend [48]. For blockchain solutions, more relevant and user-friendly applications are still needed.
- *Bitcoin's reputational risk:* There is a common misperception that BT is inextricably linked to Bitcoin and digital currencies, rather than being viewed as two distinct developments. Furthermore, speculators, profit-driven entrepreneurs, and libertarians have all been associated with Bitcoin [94, 107].
- *Social, legal, and regulatory issues to be addressed:* The socio-legal and regulatory frameworks for blockchain, containing related privacy rules, are evolving at a slower rate than the technology itself [48]. Blockchain practitioners should keep an eye on these advancements and keep up with the latest advances.

The challenges related to blockchain are presented in Fig. 3.

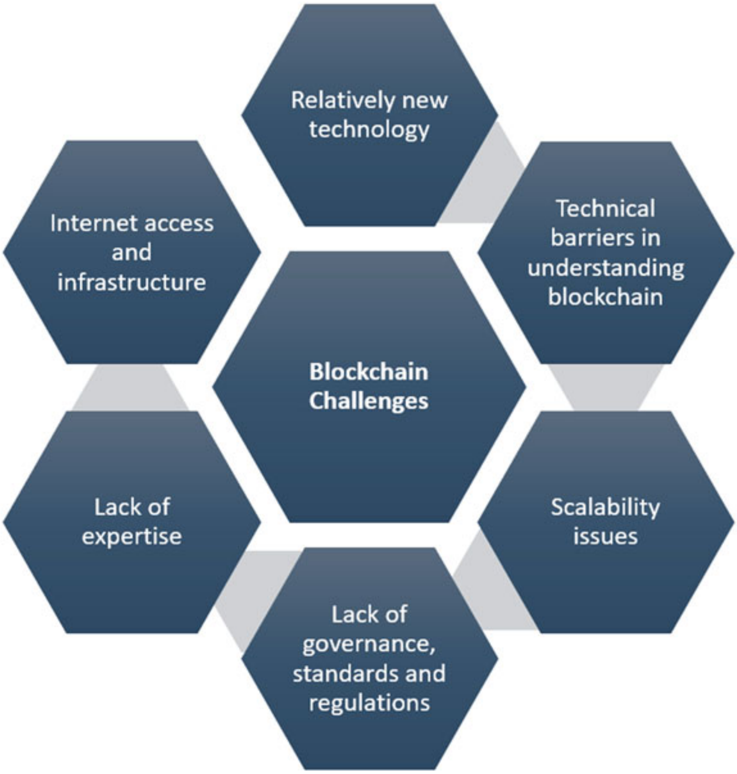

Relatively new technology
Technical barriers in understanding blockchain
Internet access and infrastructure
Blockchain Challenges
Lack of expertise
Scalability issues
Lack of governance, standards and regulations

Fig. 3 Challenges in blockchain. (Source: Author)

6 Conclusion

This study investigated the applications of BT in SCM and presented the benefits and challenges related to BT. The study answers the following research questions: (1) "what are the applications of BT to improve an organization's SC performance?" and (2) "what are the benefits and challenges of incorporating BT into the SC?" To answer these research questions, the author extensively explored the available literature on BT and SCM.

Blockchain technology provides an advanced platform for a new transparent and decentralized transactional method in organizations and industries. This technology's features improve trust by ensuring transparency in all kinds of data, goods, and financial transactions. In SCM, BT can readily deliver safe business operations. The technological platform is built on a distributed system that provides a continuous record that can be shared and made public. This technology provides more secure transaction tracking of all kinds (data and information transactions, money transactions, etc.). BT has the potential to drastically minimize human errors, additional costs, and time delays in the SC and logistics industry. Finally, by utilizing BT, the logistics and SC sector's challenges may be reduced, if not eliminated, and the organization's overall performance can be improved considerably. In the fifth section, relevant conclusions concerning prospective hurdles and benefits of BT application are drawn based on prior research. This technology facilitates SC activities such as tracking purchase orders, order modifications, and documentation of freight, as well as communicating information regarding production and delivery. BT offers enormous potential for growth and implementation in the field of logistics and SC, posing several challenges for future research.

This study adds to the literature on BT and SCM by synthesizing the literature on applications of BT. In addition, the study classified the contributions of BT to SCM performance in any firm. Even though the study addressed the two research questions, significant limitations must be considered. Firstly, the study is purely based on the available literature and the scope is limited to the application of BT in the supply chain. Secondly, papers that were assessed were mostly publications from "Scopus-indexed" journals. While Scopus is the most comprehensive database, future research may also be conducted using Web of Science, ProQuest, EBSCO, etc. How BT can be used to improve performance varies by industry. A future study needs to examine how blockchain technologies may contribute to the performance of SCs in various industries.

References

1. M.H. Ali, L. Chung, A. Kumar, S. Zailani, K.H. Tan, A sustainable blockchain framework for the halal food supply chain: Lessons from Malaysia. Technol. Forecast. Soc. Chang. **170**, 120870 (2021). https://doi.org/10.1016/j.techfore.2021.120870
2. S. Anandhi, R. Anitha, S. Venkatasamy, RFID based verifiable ownership transfer protocol using blockchain technology, in *Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August*, (Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ, 2018), pp. 1616–1621
3. I.M. Ar, I. Erol, I. Peker, A.I. Ozdemir, T.D. Medeni, I.T. Medeni, Evaluating the feasibility of blockchain in logistics operations: A decision framework. Expert Syst. Appl. **158**, 113543 (2020). https://doi.org/10.1016/j.eswa.2020.113543
4. M. Attaran, Digital technology enablers and their implications for supply chain management, in *Supply Chain Forum: An International Journal*, vol. 21, No. 3, (Taylor & Francis, 2020), pp. 158–172. https://doi.org/10.1080/16258312.2020.1751568
5. R. Azzi, R.K. Chamoun, M. Sokhn, The power of a blockchain-based supply chain. Comput. Ind. Eng. **135**, 582–592 (2019)
6. V. Babich, G. Hilary, OM Forum—Distributed ledgers and operations: What operations management researchers should know about blockchain technology. Manuf. Serv. Oper. Manag. **22**(2), 223–240 (2020)
7. H. Baharmand, T. Comes, Leveraging partnerships with logistics service providers in humanitarian supply chains by blockchain-based smart contracts. IFAC-PapersOnLine **52**(13), 12–17 (2019)

8. H. Baharmand, A. Maghsoudi, G. Coppi, Exploring the application of blockchain to humanitarian supply chains: Insights from humanitarian supply blockchain pilot project. Int. J. Oper. Prod. Manag. **41**(9), 1522–1543 (2021a). https://doi.org/10.1108/IJOPM-12-2020-0884
9. H. Baharmand, N. Saeed, T. Comes, M. Lauras, Developing a framework for designing humanitarian blockchain projects. Comput. Ind. **131**, 103487 (2021b)
10. G. Baralla, A. Pinna, G. Corrias, Ensure traceability in european food supply chain by using a blockchain system, in *Proceedings of the 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain, WETSEB, Montreal, QC, Canada, 27 May 2019*, (Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ, 2019), pp. 40–47
11. R. Beck, J. Stenum Czepluch, N. Lollike, S. Malone, Blockchain: The gateway to trust-free cryptographic transactions, in *Proceedings of the 24th European Conference on Information Systems (ECIS), Istanbul, Turkey*, (2016)
12. C. Bode, S.M. Wagner, Structural drivers of upstream supply chain complexity and the frequency of supply chain disruptions. J. Oper. Manag. **36**, 215–228 (2015)
13. M.P. Caro, M.S. Ali, M. Vecchio, R. Giaffreda, Blockchain-based traceability in agri-food supply chain management: A practical implementation, in *Proceedings of the IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Siena, Italy*, (2018)
14. R. Casado-Vara, J. Prieto, F. De la Prieta, J.M. Corchado, How blockchain improves the supply chain: Case study alimentary supply chain. Procedia Comput Sci **134**, 393–398 (2018)
15. S.E. Chang, Y.C. Chen, M.F. Lu, Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. Technol. Forecast. Soc. Chang. **144**, 1–11 (2019)
16. Y. Chen, C. Bellavitis, Blockchain disruption and decentralized finance: The rise of decentralized business models. J. Bus. Ventur. Insights **13**, e00151 (2020). https://doi.org/10.1016/j.jbvi.2019.e00151
17. T.M. Choi, L. Feng, R. Li, Information disclosure structure in supply chains with rental service platforms in the blockchain technology era. Int. J. Prod. Econ. **221**, 107473 (2020a). https://doi.org/10.1016/j.ijpe.2019.08.008
18. T.-M. Choi, S. Guo, S. Luo, When blockchain meets social-media: Will the result benefit social media analytics for supply chain operations management? Transp. Res. Part E Logist. Transp. Rev. **135**(C), 101860 (2020b). https://doi.org/10.1016/j.tre.2020.101860
19. R. Cole, M. Stevenson, J. Aitken, Blockchain technology: Implications for operations and supply chain management. Supply Chain Manage. Int. J. **24**(4), 469–483 (2019). https://doi.org/10.1108/SCM-09-2018-0309
20. M.C. Cooper, D.M. Lambert, J.D. Pagh, Supply chain management: More than a new name for logistics. Int. J. Logist. Manage. **8**(1), 1–14 (1997). https://doi.org/10.1108/09574099710805556
21. M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, Blockchain technology: Beyond bitcoin. Appl. Innovation Rev. **2**, 6–19 (2016). Available at: http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf
22. E. Demir, M.H. Bilgin, G. Karabulut, A.C. Doker, The relationship between cryptocurrencies and COVID-19 pandemic. Eurasian Econ. Rev. **10**(3), 349–360 (2020)
23. M. Dobrovnik, D. Herold, E. Furst, S. Kummer, Blockchain for and in logistics: What to adopt and where to start. Logistics **2**(3), 1–18 (2018). https://doi.org/10.3390/logistics2030018
24. R. Dubey, A. Gunasekaran, D.J. Bryde, Y.K. Dwivedi, T. Papadopoulos, Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. Int. J. Prod. Res. **58**(11), 1–18 (2020)
25. R. Dubey, A. Gunasekaran, S.J. Childe, B.T. Hazen, T. Papadopoulos, Blockchain for humanitarian supply chain, in *Supply Chain 4.0: Improving Supply Chains with Analytics and Industry 4.0 Technologies*, ed. by E. Aktas, M. Bourlakis, I. Minis, V. Zeimpekis, vol. 61, (Kogan Page Publishers, London, 2021)

26. F. Ebinger, B. Omondi, Leveraging digital approaches for transparency in sustainable supply chains: A conceptual paper. Sustainability **12**(15), 1–16 (2020). https://doi.org/10.3390/su12156129
27. M.A. Engelhardt, Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technol. Innov. Manag. Rev. **7**(10), 22–34 (2017)
28. B. Esmaeilian, J. Sarkis, K. Lewis, S. Behdad, Blockchain for the future of sustainable supply chain management in industry 4.0. Resour. Conserv. Recycl. **163**, 105064 (2020). https://doi.org/10.1016/j.resconrec.2020.105064
29. M.E. Falagas, E.I. Pitsouni, G.A. Malietzis, G. Pappas, Comparison of PubMed, scopus, web of science, and google scholar: Strengths and weaknesses. FASEB J **22**(2), 338–342 (2008). https://doi.org/10.1096/fj.07-9492LSF
30. V. Filimonau, E. Naumova, The blockchain technology and the scope of its application in hospitality operations. Int. J. Hosp. Manag. **87**, 102383 (2019)
31. B. Forde, M. Carey, The blockchain will become our new signature (Wired UK) (2016). Retrieved December 16, 2021, from www.wired.co.uk/news/archive/2016-01/05/blockchain-is-the-new-signature
32. K. Francisco, D. Swanson, The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics **2**(1), 1–13 (2018). https://doi.org/10.3390/logistics2010002
33. B. Fu, Z. Shu, X. Liu, Blockchain enhanced emission trading framework in fashion apparel manufacturing industry. Sustainability **10**(4), 1105 (2018). https://doi.org/10.3390/su10041105
34. P. Giungato, R. Rana, A. Tarabella, C. Tricase, Current trends in sustainability of bitcoins and related blockchain technology. Sustainability **9**(12), 2214 (2017). https://doi.org/10.3390/su9122214
35. A. Grech, A.F. Camilleri, *Blockchain in Education, 132 S, JRC-Science for Policy Report* (Publications Office of the European Union, Luxembourg, 2017)
36. V. Grewal-Carr, S. Marshall, *Blockchain-Enigma. Paradox. Opportunity* (Deloitte, UK, 2016). Retrieved December 16, 2021, from Delloite Website: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf
37. T. Gurpinar, G. Guadiana, P.A. Ioannidis, N. Straub, M. Henke, The current state of blockchain applications in supply chain management, in *2021 The 3rd International Conference on Blockchain Technology (ICBCT '21), March 26–28, 2021, Shanghai, China*, (ACM, New York, NY, 2021), p. 11. https://doi.org/10.1145/3460537.3460568
38. N. Hackius, M. Petersen, Blockchain in logistics and supply chain: Trick or treat? in *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23, ISBN 978-3-7450-4328-0*, ed. by W. B. Kersten, T. Ringle, M. Christian, (epubli GmbH, Berlin, 2017), pp. 3–18. https://doi.org/10.15480/882.1444
39. K.S. Hald, A. Kinra, How the blockchain enables and constrains supply chain performance. Int. J. Phys. Distrib. Logist. Manage. **49**(4), 376–397 (2019). https://doi.org/10.1108/IJPDLM-02-2019-0063
40. F. Hawlitschek, B. Notheisen, T. Teubner, The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. **29**, 50–63 (2018). https://doi.org/10.1016/j.elerap.2018.03.005
41. M. Heutger, M. Kückelhaus, Blockchain in logistics. *DHL* (2018). https://www.logistics.dhl/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf
42. IBM, What is blockchain? (2018). Retrieved from: https://www.ibm.com/downloads/cas/K54GJQJY. Accessed 15 Dec 2021
43. U. Khadke, S. Parkhi, Implementation of blockchain in the humanitarian supply chain benefits and blockades. Psychol. Educ. J. **57**(9), 5098–5105 (2020)
44. M. Khan, S. Imtiaz, G.S. Parvaiz, A. Hussain, J. Bae, Integration of internet-of-things with blockchain technology to enhance humanitarian logistics performance. IEEE Access **9**, 25422–25436 (2021)

45. A.A.A. Khanfar, M. Iranmanesh, M. Ghobakhloo, M.G. Senali, M. Fathi, Applications of blockchain technology in sustainable manufacturing and supply chain management: A systematic review. Sustainability **13**(14), 7870 (2021). https://doi.org/10.3390/su13147870
46. J.-S. Kim, N. Shin, The impact of blockchain technology application on supply chain partnership and performance. Sustainability **11**(21), 6181 (2019). https://doi.org/10.3390/su11216181
47. T. Ko, J. Lee, D. Ryu, Blockchain technology and manufacturing industry: Real-time transparency and cost savings. Sustainability **10**(11), 4274 (2018). https://doi.org/10.3390/su13147870
48. V. Ko, A. Verity, Blockchain for the humanitarian sector: Future opportunities. Digital Humanitarian Network, OCHA (2016). Retrieved December 15, 2021, from https://reliefweb.int/report/world/blockchain-humanitarian-sector-future-opportunities
49. M. Kouhizadeh, J. Sarkis, Blockchain practices, potentials, and perspectives in greening supply chains. Sustainability **10**(10), 3652 (2018)
50. L.L.P. KPMG, *Blockchain and the Future of Finance: A Potential New World for CFOs—and How to Prepare* (KPMG, Amstelveen, 2018)
51. N. Kshetri, Blockchain's roles in meeting key supply chain management objectives. Int. J. Inf. Manag. **39**, 80–89 (2018). https://doi.org/10.1016/j.ijinfomgt.2017.12.005
52. N. Kshetri, Blockchain and sustainable supply chain management in developing countries. Int. J. Inf. Manag. **60**, 102376 (2021). https://doi.org/10.1016/j.ijinfomgt.2021.102376
53. K. Kuhi, K. Kaare, O. Koppel, Ensuring performance measurement integrity in logistics using blockchain, in *Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI, Singapore, 31 July–2 August 2018*, (Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ, 2018), pp. 256–261
54. A. Kumar, R. Liu, Z. Shan, Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. Decis. Sci. **51**(1), 8–37 (2019). https://doi.org/10.1111/deci.12396
55. C. L'Hermitte, N.K.C. Nair, A blockchain-enabled framework for sharing logistics resources in emergency operations. Disasters **45**(3), 527–554 (2020). https://doi.org/10.1111/disa.12436
56. J. Leng, G. Ruan, P. Jiang, K. Xu, Q. Liu, X. Zhou, C. Liu, Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. Renewable Sustainable Energy Rev. **132**(C), 110112 (2020). https://doi.org/10.1016/j.rser.2020.110112
57. J. Leng, S. Ye, M. Zhou, J.L. Zhao, Q. Liu, W. Guo, W. Cao, L. Fu, Blockchain-secured smart manufacturing in industry 4.0: A survey. IEEE Trans. Syst. Man Cybern.: Syst. **51**(1), 237–252 (2021). https://doi.org/10.1109/TSMC.2020.3040789
58. Z. Li, H. Guo, A.V. Barenji, W.M. Wang, Y. Guan, G.Q. Huang, A sustainable production capability evaluation mechanism based on blockchain, LSTM, analytic hierarchy process for supply chain network. Int. J. Prod. Res. **58**(24), 7399–7419 (2020). https://doi.org/10.1080/00207543.2020.1740342
59. D. Liao, X. Wang, Applications of blockchain technology to logistics management in integrated casinos and entertainment. Informatics **5**(4), 44 (2018). https://doi.org/10.3390/informatics5040044
60. M.K. Lim, Y. Li, C. Wang, M.L. Tseng, A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. Comput. Ind. Eng. **154**, 107133 (2021)
61. Y.P. Lin, J.R. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, Y.F. Ho, Blockchain: The evolutionary next step for ICT e-agriculture. Environments **4**(3), 1–13 (2017)
62. L. Liu, F. Li, E. Qi, Research on risk avoidance and coordination of supply chain subject based on blockchain technology. Sustainability **11**(7), 2182 (2019). https://doi.org/10.3390/su11072182
63. V.K. Manupati, T. Schoenherr, M. Ramkumar, S.M. Wagner, S.K. Pabba, R.I.R. Singh, A blockchain-based approach for a multi-echelon sustainable supply chain. Int. J. Prod. Res. **58**(7), 2222–2241 (2020). https://doi.org/10.1080/00207543.2019.1683248

64. B. Marr. How blockchain will transform the supply chain and logistics industry. Forbes (2018), https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchainwill-transform-the-supply-chain-and-logistics-industry/. Accessed 25 Nov 2021
65. T. McConaghy, R. Marques, A. Muller, D.D. Jonghe, T.T. McConaghy, G. McMullen, R. Hendersen, S. Bellemare, A. Granzotto, BigchainDB: A scalable blockchain database (2016). Retrieved December 17, 2021 from https://git.berlin/bigchaindb/site/raw/commit/b2d98401b65175f0fe0c169932ddca0b98a456a6/_src/whitepaper/bigchaindb-whitepaper.pdf
66. H. Min, Blockchain technology for enhancing supply chain resilience. Bus. Horiz. **62**(1), 35–45 (2019)
67. M. Montecchi, K. Plangger, M. Etter, It's real, trust me! Establishing supply chain provenance using blockchain. Bus. Horiz. **62**(3), 283–293 (2019a)
68. M. Montecchi, K. Plangger, M. Etter, It's real, trust me! Establishing supply chain provenance using blockchain. Bus. Horiz. **62**(3), 283–293 (2019b). https://doi.org/10.1016/j.bushor.2019.01.008
69. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008). Accessible at: https://bitcoin.org/bitcoin.pdf. Accessed 08 Dec 2021
70. M. Nakasumi, Information sharing for supply chain management based on block chain technology, in *Proceedings - 2017 IEEE 19th Conference on Business Informatics, CBI 2017*, vol. 1, (IEEE, 2017), pp. 140–149
71. D. Namiot, O. Pokusaev, V. Kupriyanovsky, A. Akimov, Blockchain applications for transport industry. Int. J. Open Inf. Technol. **5**(12), 123–129 (2017)
72. OECD, OECD blockchain primer (2018). Retrieved from: https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf. Accessed 17 Dec 2021
73. I. Onder, H. Treiblmaier, Blockchain and tourism: Three research propositions. Ann. Tour. Res. **72**, 180–182 (2018). https://doi.org/10.1016/j.annals.2018.03.005
74. A.I. Ozdemir, I.M. Ar, I. Erol, Assessment of blockchain applications in travel and tourism industry. Qual. Quant. **54**, 1549–1563 (2019). https://doi.org/10.1007/s11135-019-00901-w
75. A.I. Ozdemir, I. Erol, I.M. Ar, I. Peker, A. Asgary, T.D. Medeni, I.T. Medeni, The role of blockchain in reducing the impact of barriers to humanitarian supply chain management. Int. J. Logist. Manage. **32**(2), 454–478 (2021). https://doi.org/10.1108/IJLM-01-2020-0058
76. E. Piscini, G. Hyman, W. Henry, *Blockchain: Trust Economy* (Deloitte University Press, 2017)., https://www2.deloitte.com/insights/us/en/focus/tech-trends/2017/blockchain-trust-economy.html
77. M. Pournader, Y. Shi, S. Seuring, S.C.L. Koh, Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. Int. J. Prod. Res. **58**(7), 2063–2081 (2020). https://doi.org/10.1080/00207543.2019.1650976
78. M.M. Queiroz, S.F. Wamba, Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. Int. J. Inf. Manag. **46**, 70–82 (2019)
79. M.M. Queiroz, R. Telles, S.H. Bonilla, Blockchain and supply chain management integration: A systematic review of the literature. Supply Chain Manag. **25**(2), 241–254 (2020)
80. A. Rejeb, J.G. Keogh, H. Treiblmaier, How blockchain technology can benefit marketing: Six pending research areas. Front. Blockchain **3**, 1–12 (2020). https://doi.org/10.3389/fbloc.2020.00003
81. A. Rejeb, K. Rejeb, S. Simske, H. Treiblmaier, Blockchain technologies in logistics and supply chain management: A bibliometric review. Logistics **5**(72), 1–28 (2021)
82. P.W. Robertson, P.R. Gibson, J.T. Flanagan, Strategic supply chain development by integration of key global logistical process linkages. Int. J. Prod. Res. **40**(16), 4021–4040 (2002)
83. M.C. Ruzafa, *Blockchain as a chain for humanitarian aid: Transforming the lives of refugees* (ISCTE Business School, Lisbon, 2020). Retrieved December 17, 2021, from https://repositorio.iscte-iul.pt/bitstream/10071/22289/1/master_marta_calsina_ruzafa.pdf
84. S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. **57**(7), 2117–2135 (2019). https://doi.org/10.1080/00207543.2018.1533261

85. R.G. Schroeder, S.M. Goldstein, M.J. Rungtusanatham, *Operations Management in the Supply Chain – Decisions and Cases*, 6th edn. (McGraw-Hill Irwin, 2013)
86. S. Schuetz, V. Venkatesh, Blockchain, adoption, and financial inclusion in India: Research opportunities. Int. J. Inf. Manage. **52**, 101936 (2020). https://doi.org/10.1016/j.ijinfomgt.2019.04.009
87. E. Seyedsayamdost, P. Vanderwal, From good governance to governance for good: Blockchain for social impact. J. Int. Dev. **32**(6), 943–960 (2020)
88. V. Shardeo, A. Patil, J. Madaan, Critical success factors for blockchain technology adoption in freight transportation using fuzzy ANP – Modified TISM Approach. Int. J. Inf. Technol. Decis. Making **19**(6), 1549–1580 (2020)
89. P.F. Skilton, J.L. Robinson, Traceability and normal accident theory: How does supply network complexity influence the traceability of adverse events? J. Supply Chain Manage. **45**(3), 40–53 (2009). https://doi.org/10.1111/j.1745-493X.2009.03170.x
90. T.F. Stafford, H. Treiblmaier, Characteristics of a blockchain ecosystem for secure and sharable electronic medical records. IEEE Trans. Eng. Manag. **67**(4), 1340–1362 (2020). https://doi.org/10.1109/TEM.2020.2973095
91. B. Sundarakani, A. Ajaykumar, A. Gunasekaran, Big data driven supply chain design and applications for blockchain: An action research using case study approach. Omega **102**, 102452 (2021). https://doi.org/10.1016/j.omega.2021.102452
92. M. Swan, Blockchain: Blueprint for a new economy. O'Reilly Media (2015). Retrieved Dec 18, 2021, from https://ahkyee.files.wordpress.com/2015/09/swan-2015-blockchain-blueprint-for-a-new-economy.pdf
93. D. Tapscott, A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (Penguin, Portfolio, 2016)
94. S. Taylor, *Blockchain: Understanding the Potential* (Barclays, England, 2015). Retrieved December 1, 2021, from https://www.weusecoins.com/assets/pdf/library/Barclays%20Blockchain%20Understanding%20the%20Potential.pdf
95. M. Tehrani, S.M. Gupta, Designing a Sustainable Green Closed-Loop Supply Chain under Uncertainty and Various Capacity Levels. Logistics **5**(2), 1–29 (2021). https://doi.org/10.3390/logistics5020020
96. F. Tian, An agri-food supply chain traceability system for china based on rfid & blockchain technology, in *Proceedings of the 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China*, (2016)
97. E. Tijan, S. Aksentijevic, K. Ivanic, M. Jardas, Blockchain technology implementation in logistics. Sustainability **11**(4), 1–13 (2019). https://doi.org/10.3390/su11041185
98. H. Treiblmaier, The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Manag. **23**(6), 545–559 (2018). https://doi.org/10.1108/SCM-01-2018-0029
99. H. Treiblmaier, Combining blockchain technology and the physical internet to achieve triple bottom line sustainability: A comprehensive research agenda for modern logistics and supply chain management. Logistics **3**(1), 1–13 (2019). https://doi.org/10.3390/logistics3010010
100. H. Treiblmaier, Blockchain and tourism, in *Handbook of E-Tourism*, ed. by Z. Xiang, M. Fuchs, U. Gretzel, W. Hopken, (Springer, International Publishing, Cham, 2020), pp. 1–21. ISBN 978-3-030-05324-6.
101. H. Treiblmaier, C. Sillaber, The impact of blockchain on e-commerce: A framework for salient research topics. Electron. Commer. Res. Appl. **48**, 101054 (2021). https://doi.org/10.1016/j.elerap.2021.101054
102. M. Turfa, *The Usage of Decentralized Applications for Enhancing the Donation Process* (Institute of Architecture of Application Systems, Germany, 2019). Retrieved December 10, 2021, from https://elib.uni-stuttgart.de/bitstream/11682/10262/1/bachelor-thesis-Turfa.pdf
103. R. van Hoek, Unblocking the chain – Findings from an executive workshop on blockchain in the supply chain. Supply Chain Manag. **25**(2), 255–261 (2020). https://doi.org/10.1108/SCM-11-2018-0383

104. V.G. Venkatesh, K. Kang, B. Wang, R.Y. Zhong, A. Zhang, System architecture for blockchain based transparency of supply chain social sustainability. Robot. Comput. Integr. Manuf. **63**, 101896 (2020). https://doi.org/10.1016/j.rcim.2019.101896
105. N. Vyas, A. Beije, B. Krishnamachari, *Blockchain and the Supply Chain: Concepts, Strategies and Practical Applications* (Kogan Page, London, 2019)
106. Y. Wang, J.H. Han, P. Beynon-Davies, Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. Supply Chain Manage. Int. J. **24**(1), 62–84 (2019). https://doi.org/10.1108/SCM-03-2018-0148
107. M. Wilson, A. Yelowitz, Characteristics of bitcoin users: An analysis of google search data. Appl. Econ. Lett. **22**(13), 1030–1036 (2015). https://doi.org/10.1080/13504851.2014.995359
108. L.-W. Wong, G.W.-H. Tan, V.-H. Lee, K.-B. Ooi, A. Sohal, Unearthing the determinants of blockchain adoption in supply chain management. Int. J. Prod. Res. **58**(7), 2100–2123 (2020). https://doi.org/10.1080/00207543.2020.1730463
109. World Economic Forum, Building Block(chain)s for a better planet. Fourth industrial revolution for the earth series (2018). Retrieved at: http://www3.weforum.org/docs/WEF_Building-Blockchains.pdf
110. J. Wu, N.K. Tran, Application of blockchain technology in sustainable energy systems: An overview. Sustainability **10**, 3067 (2018)
111. H. Zhang, T. Nakamura, K. Sakurai, Security and trust issues on digital supply chain, in *Proceedings of the 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Fukuoka, Japan, 5–8 August 2019*, (Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ, 2019), pp. 338–343.
112. W. Zheng, Z. Zheng, H.-N. Dai, X. Chen, P. Zheng, XBlock-EOS: Extracting and exploring blockchain data from EOSIO. Inf. Process. Manag. **58**(3), 102477 (2021). https://doi.org/10.1016/j.ipm.2020.102477
113. A. Zwitter, M. Boisse-Despiaux, Blockchain for humanitarian action and development aid. J. Int. Humanitarian Action **3**(16), 1–7 (2018). https://doi.org/10.1186/s41018-018-0044-5

Using Blockchain to Improve Corporate Governance

Ikram Bensalah and Aïda Kammoun Abdelmoula

1 Introduction

This chapter explores the potential of blockchain technology in corporate governance. At a time of crisis of confidence and dissatisfaction with traditional third parties and intermediaries, institutions, banks, and states, blockchain technology is emerging along with the Bitcoin phenomenon and is now on the agenda of all decision-makers. Even if the blockchain is still very little known to the general public and even if it is still difficult to precisely assess the extent of the impact that this technology will have on our society, many people already see it as the next great innovation since the emergence of the Internet. Blockchain is one of the buzzwords in the world of technology, and it has impacted many sectors. Atlam et al. [2] show that this technology, which carries the promise of disintermediation and transparency, is attractive and complicated. Blockchain promises to revolutionize the way we conduct transactions, just as the computer has changed the way we process data today and just as the Internet has transformed the way we share information at all levels. Yeretzian [28], pointed that among the first applications of blockchain technology is the cryptocurrency Bitcoin, an innovative payment network and a new form of currency that operates without a central authority; it is free and open.

According to Laurent [22], blockchain is a technology invented in 2008, made public and open source in 2009 in the same way as Bitcoin by Satoshi Nakamoto. Blockchain technology has the unique feature of allowing economic agents to

I. Bensalah (✉)
LEG, Faculty of Economics and Management Sciences, University of Sfax, Sfax, Tunisia

A. K. Abdelmoula
Higher institute of Business Administration, University of Sfax, BESTMOD Laboratory, University of Tunis, Tunis, Tunisia
e-mail: aida.kammoun@isaas.rnu.tn

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_15

abstain from intermediaries or trusted third parties to secure their transactions. The principle is simple: a blockchain is a decentralized and public history of transactions that have taken place since its creation. Its operation is based on cryptography to ensure the security of transactions and relies on the exponential development of the number and computing power of machines connected to the Internet. While the academic literature on the blockchain is just beginning to emerge, most of it focuses on the technical aspects of the technology and tends to ignore the organizational complexities of technology adoption. However, institutional, business, and technical factors interact and influence each other.

The applications of blockchain are numerous. In finance, for example, the technology can be used to trade cryptocurrencies and financial assets, to register voting rights associated with shares, to raise funds through an ICO (Initial Coin Offering) by creating equity assets associated with tokens that can be exchanged for cryptocurrencies, and to program the execution of smart contracts. Let's not forget that banks and other financial institutions, being intermediaries par excellence, may fear that their activity will be challenged by this technology, but the blockchain could strongly contribute to the reduction of the operating costs of banks in the largest sense, especially in terms of infrastructure.

Despite the extraordinary interest in blockchain, research on the subject has until recently been rather limited. Behnke and Janssen [3] and Cermeño [7] show that the emergence of modern blockchain technology has been announced as the next revolution that will change the size and structure of organizations and the way business transactions are conducted. According to Crosby et al. [9], a series of blocks can be explained by a series of date-stamped functions and a link to the previous block.

In our chapter, we ask the following question: what is the effect of the adoption of blockchain technology on corporate governance? To answer this question, we draw on the literature that focuses on the development of blockchain technology and its impact on corporate governance. Our research is more linked to Yermack [30], which focuses on the impact of blockchain adoption on various stakeholders such as executives, minority shareholders, institutional investors, and other parties. Yermack [30] states that the adoption of blockchain in corporate governance will reduce costs and improve liquidity, transparency, and accounting accuracy.

In this chapter, the first section presents the applications of blockchain technology in businesses. In the second section, we define the background of corporate governance, before specifying in the third section the relationship between blockchain and corporate governance. Finally, we analyze in the last section how blockchain impacts corporate governance based on a literature review.

2 The Applications of Blockchain Technology in Businesses

At present, there is a crisis of confidence and displeasure with traditional third parties and mediators, institutions, banks, and states. The blockchain technology that carries the Bitcoin phenomenon is currently on the agenda of all stakeholders. While blockchain is still largely unknown to the general public, and while it is still difficult to precisely appreciate the magnitude of the impact this technology will have on our society, many already see it as the next great innovation since the advent of the Internet. Blockchain technology (BT) is largely used as technical support for enterprises to enhance production processes and reduce costs [24]. The developing research offers a good opportunity to improve the performance of investment efficiency [30]. Nonetheless, there are many challenges to the perfection of BT and its application.

Blockchain technology, created in 2008, has the unique characteristic of permitting economic stakeholders to do without intermediaries or trusted third parties to secure their transactions. The principle is very simple: a blockchain is a decentralized and public history of transactions that have taken place since its creation. Its operations are based on cryptography to assure the security of transactions and rely on the exponential development of the number and computing power of machines connected to the Internet. The applications of the blockchain are multiple; in finance, the technology can be used to make exchanges of cyber-currencies and financial securities, register voting rights associated with shares, raise funds through an ICO ("Initial Coin Offering") by establishing equity securities associated with tokens that can be exchanged for cyber-currencies, and program the operation of "smart contracts." Secondly, as banks and other financial institutions are intermediaries by excellence, they may fear that their trade will be challenged by this technology. But, on the other hand, the blockchain could strongly contribute to the reduction of the operating costs of banks in the broadest sense, especially in terms of infrastructure.

2.1 Digital Payments

The blockchain has the potential to change the payment industry by enabling significant improvements in four areas: security, transaction costs, transaction times, and access to a payment method for the majority. When payment is made via the blockchain, no personal information is transmitted to the operator. In the case of a credit card transaction, the payment data is saved on a database by entities such as merchants or service providers in the area of payment. These entities then become an attractive target for hackers, feeding fraud, which in 2014 alone accounted for $16 billion worldwide.

One of the other advantages of a blockchain serving as a mode of payment is that the payments passing through it are irremediable, which can be very interesting for merchants affected by credit card fraud. Cryptocurrency payments are confirmed in a very short time. In most cases, 1 h is sufficient for the transaction to be validated and become irreversible. The money is therefore available on the merchant's account very quickly. On the contrary, credit card payments, although instantaneous on the clients' side, in reality, take several days to reach the merchant's bank account. This time lag leads to a cash flow cost for businesses that could be reduced by the blockchain. In addition, for the merchant, there is a 180-day period during which the transaction can be canceled unilaterally by the card issuer (upon request of the end customer, in case of fraud or dispute). The time for a transaction to be final is, therefore, 1 h for a cryptocurrency payment and 180 days for a credit card payment. In the same way, for individuals and small- and medium-sized businesses, an international transfer can require more than seven business days to reach its destination. During this period, on the one hand, the funds are immobilized, as they are not available to either the sender or the recipient of the transfer, and on the other hand, there is a significant exchange rate risk. Blockchain could therefore make the payment sector more efficient.

2.2 Banking

There is also another sector that could be transformed with the blockchain technology that has arrived with the promise of creating a secure environment, or decentralization and disintermediation; this is the banking sector. Banks are excited about blockchain technology. These motivations are caused by the prospects of reducing costs, reducing the risk of default and security of financial transactions, reducing delays, double spending, and standardized register.

Blockchain and, more specifically, Bitcoin were created in the aftermath of the 2008 financial crisis, which severely undermined the trust people had in financial institutions. It was therefore necessary to find a way to operate without them. This solution was found with the blockchain. Blockchain is based on the assumption that trusted third parties such as financial institutions are no longer necessary and would be replaced by a distributed consensus. Indeed, it is first of all its characteristics, at first sight perfectly implementable in the banking sector that pushed people to be interested in the blockchain.

The first element to consider is the cost of banking transactions, especially for international money transfers. As an illustration, in some countries outside the European Union, the commissions charged during the various transfers go up to ten percent of the transaction amounts, which is a considerable sum. This cost is mainly due to the various intermediaries involved in a transaction and the infrastructure required for the actual transactions.

The blockchain could then be a solution to this problem. Indeed, the cost of a transaction on the blockchain amounts to only a few cents. Thus, according to a 2015 report by Santander Bank, blockchain technology could result in a reduction in infrastructure costs for banks of $15–20 billion per year, which is a sum of approximately 17.9 billion euros. We also see through the blockchain a way to secure banking transactions and decrease the risk of default. Thanks to the traceability and transparency that the blockchain provides, we could follow money transfers from their origin to their destination, in any hand, they pass and anywhere in the world. This would, first of all, allow us to ensure the solvency of a customer but also to fight against corruption, money laundering, and terrorism financing.

This is indeed an obligation imposed on banks by the law but which is not always easy to achieve. It was enshrined in particular in the recent law of September 18, 2017, on the prevention of money laundering and terrorist financing and the limitation of the use of cash, which replaces the law of January 11, 1993, on the prevention of the use of the financial system for money laundering and terrorist financing. It should be noted, however, that some individuals may, on the contrary, use the anonymity they enjoy on these platforms for their fraudulent transactions. The European Commission intervened as early as February 2, 2016, when it published a communication on "an action plan to strengthen the fight against terrorist financing." The main idea of this communication was to force these platforms to apply vigilance measures when trading cryptocurrencies. It is feared that terrorist organizations, among others, use these virtual currency transfer platforms to hide the real origin of their financial movements, given that these transactions are recorded without being subject to reporting mechanisms as is the case for current banking systems. We can therefore see the emergence of an embryonic legal framework. However, this is more related to the regulation of Bitcoin than to the blockchain itself. We must therefore be able to ensure a balance between the effectiveness of the blockchain's registers in terms of traceability and the legal obligations of vigilance to have a system that is both effective and secure.

The problem with current online payments is that they are slow, as banks have to wait for confirmation messages before they can complete a transaction. For example, international transfers can take several days. Blockchain technology, on the other hand, makes it possible to certify a transaction almost instantaneously. For the moment, the time needed on the blockchain to validate a Bitcoin transaction is 10 min, but the Ethereum blockchain, for example, only needs 15 s to complete a transaction. This could mean that there is room for improvement to make the systems even faster. At the European level, there is also interest in this opportunity of the blockchain. Seven European banks joined forces in 2016 to set up a financing platform for the international trade of small- and med-sized enterprises (SMEs). The objective is to create a secure space in which the various actors can share information, operate transactions more easily, and use smart contracts, thus allowing a reduction in payment times.

2.3 Supply Chain

Blockchain technology can cover the broad domain of the supply chain. Supply chains are considered favored use cases for blockchain technology, as their members operate in a context of shared goals and mutual reliance. With the ability to track data from smart devices embedded in factories, depots, vehicles, and shipping sites and automatically execute payments and document delivery via smart contracts triggered by that data, blockchain concepts promise to break the trust gap that has traditionally hindered communication between members of a supply chain. As such, the technology is seen to improve efficiency, resource utilization, provenance and traceability, and credit availability.

An indicator of how effective this could be is found in the ambitions of the Hong Kong Belt and Road Blockchain Consortium (BRBC). Comprised of banks, shippers, consultants, and technology companies, the BRBC is developing a standardized system of blockchain-based business identifiers and a common dispute resolution mechanism to help make the technology the enabling platform for China's planned $1 trillion Belt and Road initiative. This massive project includes a network of advanced, intelligent manufacturing and supply chain systems in 70 different countries covering two-thirds of the world's population.

In two high-profile trials, IBM and Walmart used distributed registries technologies to track the movement of Chinese pork and Mexican mangoes along a supply chain by integrating data from farmers, produce buyers, shippers, delivery companies, wholesalers, and the retail giant itself. By making information available to chain members that would otherwise not be shared, the retailer was able to more easily identify the origin of spoiled food. Walmart, Unilever, Dole Foods, and others then joined an alliance with IBM to deploy blockchain technology for the food industry.

Similarly, blockchain startup Everledger touted its work in tracing diamonds, prompting Anglo American Ltd De Beers unit to partner with BCG Digital Ventures to do the same, in part to comply with industry rules banning diamonds from global markets war. And on the shipping side, shippers such as Maersk are working on blockchain solutions and smart contracts to streamline the processing of customs and shipping procedures.

Abeyratne et al. [1] and Kshetri et al. [19] shows that the technology Blockchain has the potential to provide solutions to problems such as those mentioned above by addressing the challenges of visibility and traceability. Blockchain technology allows companies to record every event or transaction within a supply chain (SC) on a distributed ledger, which is shared among all participants, making it secure, immutable and irrevocable.

2.4 Insurance

The insurance sector has characteristics that make it potentially susceptible to blockchain and smart contracts. The declaration and claim procedures are often tedious to fill in for the victims and costly to process for the insurance companies. Smart contracts could allow automating this administrative part and the triggering of compensations. The most obvious example is the so-called parametric insurance, which uses a parameter as a trigger. A typical farmer facing a drought will turn to their insurance company to claim compensation. A smart contract, combined with an oracle service that has access to data from the rainfall department in the area, could lead to automatic payment of compensation to all farmers concerned, without the need for any administrative formalities. This could help reduce the structural costs of insurance and increase the overall efficiency of the sector, but in the medium term, we can imagine an even more advanced use. In the continuity of companies like Uber or Airbnb, which emphasize collaborative consumption, projects have been launched to create a cooperative insurance system, without going through a classic insurance company.

Another area of insurance where blockchain could play a role is in fraud prevention. The company Everledger, for example, specializes in preventing diamond fencing by recording the unique technical characteristics of each diamond as well as its serial number on a blockchain. When a diamond is stolen or reported stolen fraudulently, it will be difficult to resell it. Also, assuming this solution is adopted on a large scale, it could stem the trade in diamonds from conflict regions. According to a note from Deloitte, using a blockchain in the car insurance industry could also reduce fraud by making it impossible to report the same claim to multiple insurance companies.

2.5 E-Government

Blockchain technology offers potential benefits for use in the public sector to improve the delivery of public services. Some of the advantages such as distribution architecture, immutability, and transparency may be useful for eradicating fraud and corruption in the public sector. With the use of technology, every transaction in public services can be recorded without manipulation and allows for better transparency and can subsequently improve trust in public services. As a result, the public sector can be more efficient and effective in its operations. Some of the advantages such as distribution architecture, immutability, and transparency may be useful for eradicating fraud and corruption in the public sector. With the use of technology, every transaction in public services can be recorded without manipulation and allows for better transparency and can subsequently improve trust in public services.

If the promised benefits of blockchain technology could be proven, it is possible that this technology could reach an inflexion point and soon begin to be widely accepted by governments around the world. However, we emphasize that these potential benefits still need to be proven through empirical evidence. Therefore, there is a need for further interdisciplinary research on broader aspects of blockchain, such as governance models, design variables, impact, and risks.

For example, Estonia is the first country to use blockchain on a national level (e-government). Indeed, it has developed its own Ksi blockchain, focused on the security of private data and the protection of networks, systems, and data. Also, Sierra Leone is the first country to use an e-voting CB for presidential elections in 2018.

Dubai: secure passports

Illinois: digitizing birth certificates

India: land registration

Gibraltar, Singapore, etc.: the creation of a regulated government cryptocurrency

3 Defining the Background of Corporate Governance

3.1 Corporate Governance Definitions

The term corporate governance came into common usage in the 1970s in the United States during the Watergate scandal, when it was revealed that US companies were involved in American politics, making contributions to various political parties. Later, in the late twentieth century, financial scandals such as Guinness 1986, Poly Peck International 1989, Maxwell 1991, BCCI 1991, Enron 2001, etc., shook the financial world and raised serious trust issues regarding corporate governance systems. The unbridled development of financial innovations, including derivatives, has contributed to the dematerialization of business operations and encouraged creative accounting practices designed to manipulate those who analyze financial statements.

So, from a historical point of view, the concept of "corporate governance" appeared in the 1970s following a series of scandals, particularly in England and the United States. The first author who manifested interest in investigating the causes of the financial disasters was Adrian Cadbury, who published the Cadbury Code. He gives the first definition of the term corporate governance as "The system by which companies are managed and controlled." Since then, several definitions were given to the term "corporate governance," and there is not a single precise definition of this term.

Table 1 presents a synthesis of several definitions.

From this table, we can remark that, in the definition of Shleifer et al. [25], the objective of corporate governance is limited to maximizing shareholder wealth. The focus is on shareholder value. However, such a definition is part of a predominantly Anglo-Saxon trend based on the predominance of the shareholder.

Other authors define this concept differently, such as Charreaux et al. [8]. In their definition, the central element is the manager (decision-making power of the company). It aims to go beyond the analysis that focuses only on the relationship between managers and shareholders. It broadens corporate governance to include stakeholders (customers, suppliers, employees, etc.) and concerns all the relationships that the company has with its many partners.

A broader definition is given by the OECD [31], "Corporate governance refers to all issues related to the separation of powers between the owners of stock firms and their managers." For Peter Wirtz [27], corporate governance is defined in this case as the set of mechanisms that delimit the discretionary space of the manager and is now recognized as an important aspect in the life of a company based on the transparency of major decisions taken and accountability to shareholders and other stakeholders.

Table 1 Some definitions for corporate governance concept

Andrei Shleifer and Robert Vishny [25]	Corporate governance refers to the way a company's funding providers ensure that they will receive the due benefits of their investment
Charreaux and Pitol-Belin [8]	"Corporate governance covers all the mechanisms that have the effect of delimiting the powers and influencing the decisions of managers, in other words, that 'govern' their conduct and define their discretionary space"
OECD [31]	"Corporate governance refers to all issues related to the separation of powers between the owners of stock firms and their managers".
OECD [32]	A set of relationships between the management of the company, the administration board, its shareholders, and some stakeholder groups
Australian National Audit Office (ANAO) [33]	"Corporate governance refers to the processes by which organizations are managed, controlled and owned. This refers to authority, responsibility, administration, management, guidance and control within the organization"
Peter Wirtz [27]	"Corporate governance specifies processes that should be adopted by managers to fulfil their duties as managers"
Marcel Ghita [34]	Corporate governance is "an attempt to implement risk analysis, verification, evaluation, control systems that contribute to efficient management for their functioning. (. . .) this has to be approached alongside risk management for the entire organization and with the evolution of the financial management and internal control system"
The United Kingdom Corporate Governance Code [35]	Corporate governance refers to "what a company's administration board does and the way it sets the company values, and it is different from day-to-day operational management by full-time managers"
Matei and Drumasu [23]	"How an organization (public or private) is lead and controlled, to accomplish its responsibilities and bring added value, as well as using financial, human, material and informational resources efficiently, while respecting the rights and obligations of all involved parties (shareholders, managers, employees, state, suppliers, clients and other people with a direct interest)"

3.2 Universal Models of Corporate Governance

From the previous section, it appears that corporate governance is the system for lining up the divergent goals of the different parties in the company and ensuring that everyone is working toward the common goal of the firm. In *shareholder governance*, the common goal is to maximize value for the owners of the company, which usually means making money for the owners. In *stakeholder governance*, the common objective is to maximize value for the different stakeholders, while recognizing that the different stakeholders define value in different ways.

According to specialized literature, there are two approaches regarding the CG involved parties:

(a) Some authors focus on shareholder value which is stakeholders who are directly involved and affected by the performance or failure of the company. In this case, various studies on corporate governance mention, in particular, the agency theory of Jensen and Meckling [36].

The agency theory is based on the potentially conflicting relationship between the owners of the company (principal) and the managers who ensure the daily management (agent). Initially, the manager is the sole owner of the company. Subsequently, an agency relationship, as well as possible conflicts of interest, is created by opening up the capital. This opening generates costs, called agency costs.

(b) More and more studies consider other stakeholders, such as managers, suppliers, state, employees, clients, banks, customers, staff members, and other persons with interests within a company. In line with this approach, several theories have been established: such as the theory of transaction costs and signal theory.

The theory of transaction costs, which is part of the theory of organizations, originates from the article of R. H. Coase published in 1937, in an article entitled "The Nature of the Firm"; the theory of transaction costs was then structured by the Nobel Prize in Economics Olivier Williamson.

For this economist, all economic transactions generate costs before their realization. Because of the uncertainties associated with them, as well as the context in which they take place, these transactions produce costs that reduce the performance of companies.

Olivier Williamson's theory begins with an analysis of the components of these transactions (called "attributes") and the structures that carry them out, the firms, which have multiple operating models (hierarchical or hybrid). From there, according to Williamson, agents become aware that saving on transaction costs is preferable to the wasteful resulting from choices guided by chance or managerial intuition. This desire to reduce costs conditions the choice of appropriate modes of governance. Finally, these governance modes serve as reference frameworks for transactions, to improve the return on investment.

The theory of signals, applied to companies, is based on the principle that the managers of a company have better information than the shareholders and the various partners of this company. A positive signal, emitted by the managers of a company, can make it possible to anticipate better future performances and to generate an increase in the share price of the value of the company and conversely.

3.3 Corporate Governance for Public Sector

The United Kingdom was among the first countries to introduce a policy of public sector governance. According to Bacon et al., the expansion of the public sector was bad for the economy. Indeed, the authors argued that an unproductive sector (the public sector) was seen as growing at the expense of a productive sector (the private sector). This led to the development of a new approach to public management when Margaret Thatcher came to power in 1979. This new form of governance assumed that private sector management techniques were far superior to the restraining principles of public administration. The application of these techniques to state entities was therefore supposed to improve the efficiency and effectiveness of the public sector. Clark [11] argues that the New Public Management (NPM) consists of three main concepts:

1. Marketization, which consists of introducing market competition into public services by separating the buyer from the supplier, creating "quasi-markets" within the public sector by tendering or outsourcing to the private sector.
2. Moving from a focus on the process to a focus on results in control and accountability mechanisms.
3. And finally, motivation, that is, creating incentives to encourage entrepreneurship, better results, and efficiency measured by performance indicators.

NPM could therefore be reduced to three M's: markets, managers, and measures. In practice, this has led to the redesign of one of England's most important public services: the health sector.

In July 1995, the Chartered Institute of Public Finance and Accountancy (CIPFA) developed the first corporate governance framework for the public sector, containing a common set of principles and standards for management and control of public organizations, organized in three fields:

- Organizational processes and structures: Discuss several aspects regarding responsibility toward the law, responsibility for public money communication with stakeholders, and roles and responsibilities for president, non-executive members of the board of directors, and executive management
- Controls and financial reporting: Consists of the following components, annual reporting, audit committees, and internal and external controls
- Behavioral standards of directors: Refers to selflessness, objectivity, integrity, accountability, openness, honesty, and leadership

In 1999, the OECD developed the key principles of corporate governance, which are:

1. Ensure the development of an adequate framework for good corporate governance. This framework should promote transparency and efficiency of markets, compliance with rules and laws, and separation of responsibilities between the different regulatory institutions and authorities.
2. Guarantee and protect shareholders' rights and key aspects of property rights.
3. Ensure equal treatment of all shareholders, including minorities and foreign shareholders. All shareholders should have the opportunity to obtain effective compensation if their rights are not respected.
4. Recognize the rights of stakeholders as set out in law or other approved commitments and encourage cooperation between organizations and stakeholders for the creation of value and jobs and to support financially sound enterprises.

5. Issue/transmit credible and timely information on all matters concerning the company, including the financial situation, performance, ownership, and management of the company.
6. Define the responsibilities of the board of directors, namely, the strategic direction of the company, the management control, and its accountability to the shareholders and the company.

4 The Relationship Between Blockchain Technology and Corporate Governance

4.1 Theoretical Basis

The main premise of this technology is new governance, both for public and private sectors, based on innovative principles: collaboration, decentralization, and transparency.

Blockchain technology can provide intelligent solutions to corporate governance issues, especially in the relationship between shareholders and companies. Operators of the technology, such as companies that may be listed on a blockchain exchange, have many reasons to worry about the governance of the blockchain itself. Open public blockchains run autonomously by computer software. This code specifies the basic inputs for each transaction, the timing and priority of encoding those transactions into the blockchain, and limits on the sizes or contingencies associated with each transaction, among other issues.

The use of blockchains ensures transparency and immutability, as transactions cannot be altered or deleted. Users have the certainty that transactions will always be executed according to the agreed protocol, ensuring the integrity of the process and thus ensuring complete, consistent, accurate, and timely data. In the case of an asset (a house for example), it is, therefore, possible to trace it from the beginning, eliminating the risk of counterfeiting or duplicate sales, since blockchain users can ensure that the person who claims to own an asset does own it.

Eventually, blockchains could contribute to a significant reduction in unit transaction costs as the involvement of a trusted intermediary would no longer be necessary. And that is the main innovative character of this technology which persuades some hopeful future-orientated people that traditional banks, auditors, brokerage houses, and many such intermediaries will soon disappear.

Several concrete benefits can be obtained from the adoption of blockchain technology in the public sector, especially if we talk about collaboration between public administrations. In fact, blockchain is a technology that allows different actors to coordinate with each other, so it may lead to new governance systems based on more collaborative models. This could make it easier for public administration structures, which are highly dependent on each other, to work together. It is possible to group and federate the activities of different structures without having to bear the cost and complexity of creating a central entity to govern the relationships between actors. Here, blockchain can help foster collaboration, creating network effects, new synergies, and a more collaborative and participatory working environment, based on shared trust. This could remove redundant tasks of data verification and duplication of processes through the sharing of a common source validated and accepted as such by all parties. Giving the example of the attempt launched by the German government in the region of Zug to use blockchain technology to assign a digital, decentralized and sovereign identity to each of its citizens, it allows them to take part in government-related activities such as getting checked by local authorities, voting and using public services.

In addition, the use of blockchain enhances transparency and trust as there is no "single" owner of the data in the shared register, and it makes it easier to identify and quantify the benefits for each of the administrations involved since the common interest and the service of the user are the main values shared by the participants.

Finally, fraud, violation of information, and data confidentiality are problems for government data operations. The silos within different government parts result in multiple versions of multiuser data. Without a single version, the risk of fraud and the difficulty of ensuring conformity increases each time a dataset is accessed, as there is no way to distinguish correct from incorrect entries. Blockchain technology could provide the solution by creating a shared and trusted database ledger that is sequentially adding data cryptographically secured. This assures government administrators that they are working with up-to-date, accurate data that is virtually impossible to manipulate.

4.2 Potential Uses of Blockchain Technology by Financial Sector for Better Governance

Blockchain technology seems to have great potential in financial activities and particularly in financial markets. The main reasons are the expected decrease in transaction costs due to the reduction in the number of intermediaries and the security of transactions.

4.2.1 Primary Market Activities

Beyond the technology as an exchange system, the blockchain has also found through cryptocurrencies a use as a means of raising funds, in place of both traditional stock exchanges and the private equity market.

For several months now, new public offerings have been successful in the United States and elsewhere; they are carried out in the form of cryptocurrencies, such as Bitcoin (BTC) or Ether (ETH). Hence their name is Initial Coin Offering (ICO), like the Initial Public Offering (IPO).

These operations are a fast mode of financing; it takes a few days to a few hours to raise the funds.

Among the characteristics of ICOs and the differences with traditional fundraising, we can note the following:

- Investors often do not need to identify themselves on the platform.
- The amount raised is transparent: BTC and ETH payments are recorded on public blockchains, which allows anyone to see the amount and amounts going to an ICO address. However, although the amounts invested are transparent, it is almost impossible to know if the project is a real success or if the fundraising is artificial due to the presence of the issuer itself in the raising.
- There are sometimes minimum and maximum total fundraising amounts. If the minimum is not reached, the investors are reimbursed and the project does not continue. When the maximum is reached, no more tokens are distributed.

4.2.2 Means of Payment

When a payment is issued through the blockchain, no personal information is transmitted to the merchant. On the other hand, in the case of a credit card transaction, the payment data is recorded on a database by entities such as merchants or service providers in the field. These entities then become targets for hackers, and fuel fraud, the amount of which in 2014 alone reached $16 billion globally.

Another advantage of a blockchain serving as a means of payment is that cryptocurrency payments are validated in a very short time. In the majority of cases, 1 h is enough for the transaction to be confirmed and irreversible. The money is therefore available in the merchant's account very quickly. In contrast, credit card payments, although instantaneous on the customer's side, actually take several days to reach the merchant's bank account. This time lag leads to a cash flow cost for businesses that could be reduced by the blockchain. Similarly, for individuals and small- and medium-sized businesses, an international transfer can take more than seven working days to reach its destination. During this period, on the one hand, the funds are immobilized, as they are not available to either the sender or the recipient of the transfer, and, on the other hand, there is a significant exchange rate risk. Blockchain could therefore make the payment sector more efficient.

4.2.3 Automation of Procedures

The invention of blockchains and smart contract programs could have a strong impact on the financial sector by allowing the automation of certain procedures, contributing to the reduction of costs and risks, particularly counterparty risk. Counterparty risk is the risk that a business partner is unable or unwilling to meet its commitments for one reason or another. For example, a company or government experiencing poor economic conditions may decide to unilaterally defer payment of its debts. If the terms of a contract are clearly defined in a smart contract, which is itself registered in a blockchain, the execution of the contract becomes unavoidable, regardless of the degree of honesty of the parties involved. The notion of ambiguity then disappears completely, thus reducing the risk of the counterparty. The reduction of costs comes again from the possibility of abstaining from intermediaries.

We can thus distinguish several areas that could be affected by automation of procedures. These areas are financial transactions, crowdfunding, insurance, and supply chains.

– Financial transactions

The automation of financial transactions is an innovation of particular interest to banks. Deutsche Bank has revealed that it is researching to develop a smart bond project whose characteristic is that coupons are automatically deducted from the borrower and credited to the lender by the smart contract.

We can further imagine smart contracts on derivatives, whose post-trading process would be carried out automatically. The smart contract could thus automatically trigger the payment of margins, continuously throughout the day, draw down the account of the party concerned, and close when one of the counterparties defaults. By reducing the counterparty risk in this way, the services of clearinghouses could become superfluous. All contract data (amount, involved parties, duration, etc.) are recorded in the blockchain, becoming then a database that could be consulted by regulators.

– Crowdfunding

Crowdfunding is an alternative means of financing that aims to allow companies, especially startups, to finance themselves directly from individuals. The objective is to short-circuit the classical way by avoiding banks, which allows reducing the cost of financing. It is even in some cases the only possible source of financing, in cases where banks are reluctant to grant credits. Blockchain and smart contracts allow investors to go into the field of crowdfunding by allowing direct financing between individuals and companies.

– Insurance

The insurance sector presents characteristics that make blockchain and smart contracts potentially useful for it. Indeed, the declaration and claim procedures are often tedious to complete for the victims and costly to process for the insurance companies. Smart contracts could allow automating this administrative part and the triggering of compensations. In the continuity of companies like Uber or Airbnb, which promote collaborative consumption, projects have been launched to create a cooperative insurance system, without going through a classic insurance company.

– Supply chain management

There are four main strategies on how to use the basic idea of blockchain technology to improve supply chains themselves or develop new business models.

– Improve transparency:

- Authenticate products
- Secure the traceability of certificates
- Reduce the audit burden required by internal systems and processes
- Understand product characteristics
- Facilitate collaboration
- Provide end-to-end data on your location in the supply chain
- Simplify and automate invoicing and payments
- Easily streamline processes
- Facilitate manufacturer-based (rather than distributor-based) reward programs

4.2.4 The Impact of Blockchain on the Banking Sector

The banking sector could see itself transformed with blockchain technology that can promise of creating a secure environment, or decentralization and disintermediation. This is due to the prospects of lowering costs, reducing the risk of default and security of financial transactions, and reducing delays. Blockchain and, more specifically, Bitcoin were created in the aftermath of the 2008 financial crisis, which severely damaged the trust people had in financial institutions. It was therefore necessary to find a way to operate without them. This solution was found with the blockchain which is based on the assumption that trusted third parties such as financial institutions are no longer necessary and would be replaced by a distributed consensus. Indeed, this idea of eliminating the intermediaries traditionally necessary for financial transactions, such as payments, leads some to believe that banks, as we know them today, are doomed to disappear.

5 Empirical Literature Review

This section presents a literature review on the effect of blockchain technology on several aspects of corporate governance

5.1 Blockchain Technology

Kristoffer and Swanson [13] study the relationship between blockchain technology and underlying value factors and use a conceptual model based on UTAUT. The results show that the factors of performance, social influence, and trust act positively on blockchain technology.

Holotiuk and Moormann [16] consider that the adoption of blockchain organizational technology depends on factors of technology, project management, environment, people, and organization using a data triangulation methodology based on interview data and archival data by conducting in-depth interviews in 11 cases with experts leading to the adoption of blockchain. The objective is to better understand the organization and adoption to explore the factors that influence adoption. The results show that the technology can replace existing technologies and the adoption of this technology is not an organization but rather an ongoing process.

Carter et al. [5] examined the adoption of public blockchain using a review on 354 items. The results show that blockchain application adoption in e-government is still very limited and there is a lack of empirical data.

Grover et al. [14] propose a conceptual framework for blockchain technology adoption capturing the complex relationships between institutional, market, and technical factors; this framework shows that different outcomes are possible and the factors interact with each other. The results show us that the organization is impacted by the adoption of blockchain.

With the enlarged research devoted into the exploration of the potential business opportunities of blockchain technology adoption, the advantages of using this technology become more recognizable and clear.

5.2 Blockchain and Corporate Governance

At the moment, blockchain technology is one of the most discussed topics. Some recent research discusses its impact on corporate governance; there is a vast and growing literature on the effect of blockchain technology, but very few studies explore the applications of blockchain, especially in corporate governance. Our study is most relevant to Yermack [30], which focuses on the impact of blockchain adoption in corporate governance on different stakeholders such as managers, small shareholders, institutional investors, and other parties. Yermack [30] finds that the adoption of blockchain in corporate governance would lead to reduced costs, increased liquidity, transparency, and accounting accuracy. Our study differs from these articles and prior literature in several respects.

The applications of blockchain technology are numerous. Record-keeping via blockchain can solve the problems associated with companies' inability to keep accurate and timely records of who holds their shares, thereby reducing settlement time. According to CPA Canada and AICPA [37], "Blockchain technology has the potential to impact all recordkeeping processes, including the way transactions are initiated, processed, authorized, recorded and reported." Blockchain offers new opportunities to simplify the agency relationship between participating companies, generating trust and transparency. Yermack [29] and Lepore et al. [21] believed that blockchain presents a high degree of increased accuracy, efficiency, and transparency in shareholding, corporate voting, and record keeping.

Bradley [12] argues that the use of blockchain significantly reduces illegal corporate practices. Lafarre and Van der Elst [20] assume that for shareholders, blockchain could offer lower trading costs and more transparent ownership records while allowing visible real-time observation of share transfers from one owner to another. Besides, according to Kahan and Rock [18], the adoption of blockchain to record stock ownership could solve many long-standing problems associated with the inability of organizations to maintain accurate and timely records of who owns their stock.

Nakasumi [41] shows that a decentralized platform improves and facilitates the decision process of storing sensitive data. Also, Kshetri [19] states the need to develop blockchain solutions in supply chains with the argument of its current dependence on the Internet of Things. The current way of sharing information between parties within the supply chain is mainly through enterprise resource planning (ERP) systems such as SAP. According to Casey and Wong [38], blockchain technology allows supply chain partners and stakeholders to identify bottlenecks in product flow. The system can detect if products have been sitting in one place for too long or in the wrong location, which is especially important for refrigerated goods. Queiroz Maciel et al. [39] examined the impact of blockchain technology on supply chain adoption using the PLS-SEM model in a transnational context (in India and the United States). The results suggest that trust among supply chain actors is not affecting blockchain adoption.

Caldero et al. [4] argue that blockchain offers partners the ability to operate securely without the intervention of a central authority or any intermediary. This enables the broader development of peer-to-peer economies and provides opportunities for a wide range of applications, from e-commerce to corporate governance.

Catalini et al. [6] affirm that integrating various bank ledgers via blockchain would speed up processes and reduce costs. However, Cong et al. [40] find that smart contracts may lead to an increase in collusive behavior among participants. Several studies explore payment system applications for blockchain.

According to Kaal [17], the Blockchain allows companies and other forms of business organizations to be complemented by agency constructs that build on this technology. Thus, blockchain-based Decentralized Autonomous Organizations (DAO) governance enables dynamic regulatory features that facilitate decentralized regulatory solutions.

6 Conclusion

Blockchain technology has revolutionized almost every sector of the business world. Whether it is banking, insurance, general management, or marketing, it is being touted as the key symbol of the fourth industrial revolution and one of the biggest disruptors for many industries [4]. Blockchain technology can not only transform the organizational culture but also increase trust between different stakeholders. The main objective of the study was to demonstrate how blockchain technology can be useful in the context of corporate governance. We can see that all aspects of corporate governance can be improved as a result of the adoption of blockchain, namely, improving efficiency by eliminating the administrative burden, guaranteeing greater transparency, minimizing the risk of fraud for organizations by providing a complete audit trajectory, and enabling efficient and easy collaboration between different government entities.

The technology has the potential to revolutionize the governance system. This chapter also highlights the opportunities for the adoption of blockchain technology at the governance level involving aspects of management, oversight, and accountability. The chapter's findings also align with available research [10, 12, 15, 20, 26] and suggest that corporate governance could change and benefit in different ways from the adoption of blockchain technology.

References

1. S.A. Abeyratne, R.P. Monfared, Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **1**(10), 5–9 (2016)
2. H.F. Atlam, G.B. Wills, Technical aspects of blockchain and IoT, in *Role of Blockchain Technology in IoT Applications*, vol. 115, (Elsevier, 2019), pp. 1–39
3. K. Behnke, M.F. Janssen, Boundary conditions for traceability in food supply chains using blockchain technology. Int. J. Inf. Manage. **52**(9), 101969 (2019). https://doi.org/10.1016/j.ijinfomgt.2019.05.025
4. M. Caldero, S. Lawrence, S. Churchil, Distributed ledgers: A future in financial services? J. Int. Banking Law Regul. **31**(5), 246–247 (2016)
5. G. Carter, D. White, A. Nalla, H. Shahriar, S. Sneha, Toward application of blockchain for improved health records management and patient care, in *Blockchain in Healthcare Today*, vol. 2, (2019). https://doi.org/10.30953/bhty.v2.37
6. C. Catalini, J.S. Gans, Some simple economics of the blockchain, *NBER Working Paper* n°22952 (2016), Available at: http://www.nber.org/papers/w22952. Revised June 2019
7. J.S. Cermeño, Blockchain in financial services: Regulatory landscape and future challenges for its commercial application, *BBVA Working Paper* n° 16/20, 33 (2016)
8. G. Charreaux, J.P. Pitol-Belin, La théorie contractuelle des organisations: une application au conseil d'administration, Le gouvernement des entreprises, Economica. 165–192 (1997). 33 pages
9. M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman, Blockchain technology: Beyond bitcoin. Appl. Innovation Rev. **2**, 5–19 (2016)
10. Cygnetise, Blockchain as a tool for corporate governance (2018), available at: www.cygnetise.com/blog/blockchain-as-a-tool-for-corporategovernance
11. D. Clark, Open government in Britain: Discourse and practice. Public Money Manage. **16**(1), 23–30 (1996)
12. F. Bradley, Blockchain comes to corporate governance with AST proxy voting (2017). Available at: http://www.nasdaq.com/article/blockchain-comes-to-corporategovernance-with-ast-proxy-voting-cm791465
13. F. Kristoffer, D. Swanson, The supply chain has no clothes: Technology adoption of blockchain for supply chain transparency. Logistics **2**(2), 1–13 (2018)
14. P. Grover, A.K. Kar, M. Janssen, P.V. Ilavarasan, Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions–insights from user-generated content on Twitter. Enterp. Inf. Syst. **13**(6), 771–800 (2019). https://doi.org/10.1080/17517575.2019.1599446
15. F. Haque, Ownership, regulation and bank risk-taking: Evidence from the Middle East and North Africa (MENA) region. Corporate Governance **19**(1), 23–43 (2018)

16. F. Holotiuk, J. Moormann, Organizational adoption of digital innovation: The case of blockchain technology, in *Proceedings of the European Conference on Information Systems, Portsmouth*, (2018)
17. W.A. Kaal, Blockchain-based corporate governance. Stanford J. Blockchain Law Policy **4**(1), 10–19 (2021)
18. M. Kahan, E.B. Rock, Hedge funds in corporate governance and corporate control. Univ. Pennsylvania Law Rev. **155**(5), 1021–1093 (2007)
19. N. Kshetri, Blockchain's roles in meeting key supply chain management objectives. Int. J. Inf. Manag. **39**, 80–89 (2018)
20. A. Lafarre, C. Van der Elst, Blockchain technology for corporate governance and shareholder activism. *TILBURG LAW SCHOOL*, Tilburg Law School Legal Studies Research Paper Series No. 07/2018, 33 (2018)
21. C. Lepore, M. Ceria, A. Visconti, U.P. Rao, K.A. Shah, L. Zanolini, A Survey on Blockchain Consensus with a Performance Comparison of PoW, PoS and Pure PoS. Mathematics **8**(10), 1–26 (2020). https://doi.org/10.3390/math8101782
22. M. Laurent, La blockchain est-elle une technologie de confiance, in *Claire Levallois-Barth. Signes de confiance: l'impact des labels sur la gestion des données personnelles, Institut Mines-Télécom*, (2018), pp. 179–198, 978-2-9557308-4-3. ffhal-01778949f
23. A. Matei, C. Drumasu, Corporate Governance and public sector entities. Procedia Econ. Finance **2**(6), 495–504 (2015)
24. D. Pan, S. Li, Z. Xu, Y. Zhang, P. Lin, H. Li, A deterministic-stochastic identification and modelling method of discrete fracture networks using laser scanning: Development and case study. Eng. Geol. **262**, 105310 (2019). https://doi.org/10.1016/j.enggeo.2019.105310
25. A. Shleifer, R.W. Vishny, A survey of corporate governance. J. Financ. **52**(2), 737–783 (1997)
26. D. Tapscott, A. Tapscott, *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*, Portfolio Edition (Penguin, 2016)
27. P. Wirtz, Meilleures pratiques de gouvernance, théorie de la firme et modèles de création de valeur: Une appréciation critique des codes de bonne conduite, *Working Papers CREGO* 1040401, Université de Bourgogne – CREGO EA7317 Centre de recherches en gestion des organisations (2004)
28. A. Yeretzian, *La blockchain décryptée, les clefs d'une révolution* (Netexplo, Paris, 2016)
29. D. Yermack, Is bitcoin a real currency? An economic appraisal (2014). Available at SSRN: https://ssrn.com/abstract=2361599 or https://doi.org/10.2139/ssrn.2361599
30. D. Yermack, Corporate governance and blockchains. Rev. Finance **21**(1), 7–31 (2017)
31. OECD, Corporate governance and corporate performance, DSTI/IND/(98)13 (1998)
32. OECD Annual Report 2001, https://doi.org/10.1787/annrep-2001-en
33. Australian National Audit Office ANAO (2003), Public Sector Governance, Volume 1, Better Practice Guide (Framework, Processes and Practices), https://www.muskratfallsinquiry.ca/files/P-01782.pdf. (page 6)
34. M. Ghiță, *Corporate governance* (Economic Publishing House, Bucharest, 2008)
35. United Kingdom Corporate Governance Code, (2012), https://www.frc.org.uk/getattachment/e322c20a-1181-4ac8-a3d3-1fcfbcea7914/UK-Corporate-Governance-Code-(September-2012).pdf
36. M.C. Jensen, W.H. Meckling, Theory of the firm: managerial behavior, agency costs and ownership structure. J. Finan. Econ. **3**(4), 305–360 (1976)
37. American Institute of Certified Public Accountants and the Chartered Professional Accountants of Canada (AIPCA and CPA Canada), (2017), Blockchain technology and its potential impact on the audit and assurance profession. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf
38. M. Casey, P. Wong, Global supply chains are about to get better, thanks to blockchain. Harv. Bus. Rev. **13**, 1–6 (2017)

39. Queiroz, S.F.. Wamba, réf 56 (2019)
40. L.W. Cong, Z. He, Blockchain disruption and smart contracts. Rev. Financ. Stud. **32**(5), 1754–1797 (2019). https://doi.org/10.1093/rfs/hhz007
41. M. Nakasumi, Information sharing for supply chain management based on block chain technology. *IEEE 19th conference on business informatics (CBI)*, pp. 140–149 (2017)

Blockchain Security as "People Security": Applying Sociotechnical Security to Blockchain Technology

Kelsie Nabben

1 Introduction

Blockchain is forecast by some to be "future of financial and cybersecurity," with the potential to "revolutionize applications and redefine the digital economy" [1]. Blockchains hold great promise to re-instate "trust" in society by enabling coordination without relying on trusted third parties [2]. If this is the case, then it is imperative to develop blockchains into functional, digital institutional infrastructure with not just transparent but legible rules of governance, operation, and security. Yet, it is rarely acknowledged that security in blockchains is contextual, according to the type of blockchain architecture, the governance model, the needs of the participants using the system, and the context in which it is being applied. Beginning from the premise that blockchains are sociotechnical systems, this chapter explores the question: "What security guarantees do different types of blockchain-based systems offer people?". The aim of this analysis is to apply a sociotechnical security approach to blockchains to clarify the expectations, assumptions, and security guarantees for those participating in blockchain infrastructure, in order for this technology to more accurately meet the needs and expectations of people. By adopting a sociotechnical security analysis framework, this chapter argues that both public and private blockchains have security shortcomings at the social, technical, and infrastructural layer. Given the sociotechnical nature of blockchain-based systems, this sociotechnical security approach is termed "people security." For private blockchains, these trust and security issues are evident in macrosocial (societal) applications. For public blockchains, security issues are present at the micro- (individual) and meso- (organizational) levels and unknown at the macrosocial level

K. Nabben (✉)
RMIT University, Melbourne, VIC, Australia
e-mail: kelsie.nabben@rmit.edu.au

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4_16

as there is a lack of suitable desktop case studies by which to analyze security in broader, social applications. These “people security” findings are important as the sociotechnical security gaps of different types of blockchains across different applications are underexplored, despite the increasing prominence of blockchain-based systems in organizations and society.

1.1 Structure of the Chapter

First, this chapter defines blockchains as a sociotechnical construct and outlines the different types of blockchains and the traditional promises of “blockchain security.” Then, it adopts a sociotechnical security lens to frame “blockchain security” as “people security” and applies a sociotechnical security approach to both public blockchains and private blockchains (“Applying Sociotechnical Security to Blockchains” section). Here, it becomes evident that both public and private blockchains hold inherent security limitations in terms of technical security, trust in social processes, and infrastructural dependencies. This chapter finds that although public blockchains afford users with a greater participatory role in technical and governance processes, private blockchains are more commonly being adopted in contexts as macrosocial coordination systems, resulting in inherent security limitations for users of these systems through centralization and lack of ownership or participation in governance processes (“Observations and Findings” section). If blockchains are to become any closer to fulfilling their promise as “tools of trust” to offer more secure institutional infrastructures in society, a sociotechnical “people security” approach is essential (“In Code We Trust? The Limitations of Security in Blockchains” section). Further research directions are then proposed to extend this theoretical framework (“Conclusion and Further Directions” section).

1.2 Methodology

This chapter adopts a science and technology studies (STS) methodology to analyze blockchains as interdisciplinary sociotechnical systems that are co-constructed in relations between the technology itself and the “real-world” social processes, norms, and application in various forms of organizations [3]. The approach is grounded in a social-constructivist view of security in sociotechnical systems, to reflect on the narrower technological determinist perspective which dominates much of the current discourse on blockchain security. Sociotechnical studies allow us to view cryptoeconomic organizing technologies as complex social systems that operate at three primary levels: the work systems level, the whole organization level, and the macrosocial system. Eric Trist first described sociotechnical systems, in the context of the coal mining industry, as micro-level work practices, meso-level organizational practices, and macro-level social systems [4]. All three of these “multiscale” levels are apparent in the organizational capabilities of blockchains as complex systems, in the actions of individual agents, the system-level setting of objectives, and the structural, system level [5]. Hayes suggests that blockchain-based cryptoeconomic systems should not be studied as money but as systems that organize individuals through the radical disintermediation of institutions [6]. Thus, employing STS methods is a suitable approach to reveal the implicit and embedded technical, social, economic, and political assumptions and decisions that influence how blockchains are applied in social contexts [7].

A sociotechnical security framework will be applied to analyze how understandings of blockchain security can evolve to consider "people security." This framing broadens existing technical approaches to inspect the social layer (people and processes), the software layer (code and applications), and the infrastructure layer (physical and technological infrastructure) [8]. This sociotechnical approach to blockchain security is termed "people security." I then draw on qualitative, digital ethnography research insights to examine a number of case studies of both public and private blockchains to test the people security approach.

1.3 Key Contributions

1. Framing of blockchains as a sociotechnical construct and multiscale institutional infrastructure that operates at micro-, meso-, and macrosocial levels across different implementations
2. A sociotechnical analysis of the security attributes and limitations of blockchain security for people across various types of blockchains and blockchain applications, to expose the trust assumptions and security issues
3. An analysis of the security assumptions for participants across different types of blockchain applications, including possible future risks from blockchain automation and why blockchain may not be a desirable digital infrastructure in macrosocial contexts

2 Blockchains as a Sociotechnical Construct

The innovation of public blockchains is the application of cryptoeconomic mechanisms to facilitate coordination at each level of a complex, sociotechnical digital system. At the technical level, blockchains incorporate the encoding of economic game theory mechanisms of byzantine fault tolerance and governance rules to enforce certain attributes, such as Sybil resistance, execute transactions, and perform certain functions as part of a broader system. At an organizational infrastructure level, blockchains are responsible for coordination within a system. At a macrosocial level, blockchains operate as a coordinating infrastructure at the social, economic, and political level in society [9]. This is why a deeper understanding of the security affordances and limitations of this digital infrastructure for the people that use it is imperative.

Blockchain security in a cybersecurity sense tends to consider blockchains as a technical object of inquiry, when, in fact, they are a sociotechnical construct [6]. Blockchains are comprised of both software code, hardware, developers, maintainers, users, standards, policy frameworks, and social processes. Blockchains enable transactions between participants in a network. They can be centrally issued and administrated (“permissioned” or “semi-permissioned”), such as private and consortium blockchains, or public and “permissionless.” The key attributes of both public and private blockchains demonstrate the ways in which security is both a technical and a social consideration.

3 Different Types of Blockchains

Blockchain technologies can be divided into three broad categories. These distinctions are important for understanding the role of people in the system and how the system operates in the context in which it is applied.

3.1 Public Blockchains

Public blockchains emphasize transparency and participation. The consensus of transactions is “decentralized,” in that anyone can participate in validating transactions on the network, and the software code is publicly available or “open-source.” Examples include Bitcoin and Ethereum.

Through their technical attributes, public blockchains offer the unique ability to provide decentralized consensus. Public blockchain networks pursue distributed consensus through “cryptoeconomics” or digital tokens to align incentives and ensure cooperation in a distributed network. In this case, “decentralization” refers to the characteristic of having no political center of control and no architectural central point of failure in the design of the software system [10]. The degree to which a blockchain is decentralized depends on the design of the consensus algorithm, issuance of cryptoeconomic incentives, ownership of cryptographic “private keys,” and governance of the network. Governance considerations include who can develop the software code, who can participate in the consensus mechanism, and who can take part in ownership and governance processes to maintain the network. The consensus mechanisms of the dominant blockchains by market capitalization, Bitcoin and Ethereum, are “proof-of-work” (PoW) or “proof-of-stake” (PoS). These unique attributes are why blockchain is ideologically conceived of as an infrastructural solution for self-governance, to address macrosocial coordination problems in society [11].

3.2 Private Blockchains

Private blockchains mean that participation in validating transactions on the network is restricted to only include parties that are approved members by a central administrator. Thus, private blockchains are centralized and operate more closely to a traditional database or governance structure.

Private blockchains often employ a "proof-of-authority" (PoA) consensus approach, meaning only approved authorities, or a single authority, can participate in validation [12]. Transaction data is most often kept private, making private blockchains more suitable for internal, secure environment business needs, such as access, authentication, and record keeping.

3.3 Consortium Blockchains

Consortium blockchains are comprised of participants that are known to one another and preapproved by a central authority to participate in consensus mechanisms in a blockchain network. This "semi-permissioned" approach allows for a network to be distributed, or partly decentralized, while allowing for a degree of control over a network between participants.

Consortium blockchains can reach consensus via PoW, PoS, PoA, or other consensus mechanisms, such as delegated proof-of-stake and more. Transaction data may be kept private. This type of blockchain may be used between known parties, in supply chain management, banking, or Internet of Things (IoT) applications.

4 Security in Different Types of Blockchains: Surfacing Assumptions

Blockchain security research is deeply focused on the technical attributes of security, which are under continuous development and improvement to strive toward the goal of offering stronger security guarantees to users [13]. All blockchains rely on secure software code to enable peer-to-peer transactions through the use of digital currency to offer security to users. A number of blockchain cybersecurity vulnerabilities remain under active investigation in the field of computer science [14].

What security means for users of a blockchain network is different across different disciplines. While cybersecurity focuses on securing networks against external threats, sociotechnical security focused on securing people, as participants in the network.

Public blockchains are often referred to as decentralized, transparent, autonomous, immutable, and pseudonymous [10]. Transactions are executed by software code in "smart contracts" or rules that govern the network [15]. According to the game theory of "cryptoeconomics," economic incentives align the interests of participants for cooperation within the network. Ownership of these cryptographically secure digital assets makes it very expensive to tamper with the network and prevent "double-spending" the same digital assets in the network, despite distributed computation of transactions between unknown parties [16]. The broader "consensus algorithms" that secure the network against cooption or "forking" of the ledger of transaction history via a 51% attack to control the network differ depending on the design of the particular blockchain network [17].

Thus, the fundamental threat which "blockchain security" protects against in public blockchains through technical characteristics and economic consensus mechanisms is the threat of centralization. The attribute of decentralization in public blockchains refers to freedom from relying on central intermediaries in its original interpretation from the cypherpunk culture and cryptoanarchic politics from which Bitcoin, the first fully functioning decentralized public blockchain, emerged [18].

In contrast, when information and validation on a blockchain are limited to certain parties, as with private and consortium blockchains, the privacy and security guarantees for users of that chain become very different. On private and permissioned blockchains, transactions can be censored through corruption or collusion, rules can be altered without the consent of users, and the administrator owns the digital assets of users if they hold the cryptographic "keys" to that data. Storage and computation may be distributed, but the "nodes" (people that run software code) that validate transactions are known to other parties in the network [1]. Thus, the authority to govern is not decentralized. These design and governance attributes have critical security implications for the assumptions of people that participate in the network if blockchains are applied as a coordination system in society but still controlled by a central issuer of digital tokens and administrator of the system.

Understanding the type of blockchain, who is being trusted in its operation and maintenance, the context in which the blockchain is being applied, and the expectations and needs of participants is vital in reframing blockchain security for sociotechnical settings.

5 Applying Sociotechnical Security to Blockchains

Sociotechnical security allows for a broader security analysis lens, encompassing the social, technical, and contextual aspects of a digital system. These aspects are integral to studying the security of blockchains as macrosocial governance infrastructure in society. This lens allows us to reframe "blockchain security" from referring to "decentralization from trusted third parties" to "people security," which considers the expectations and the needs of users as participants in blockchain-based systems.

A sociotechnical analysis is particularly valuable in analyzing blockchain systems in macrosocial contexts. People depend on "macrosocial" institutional infrastructure, such as financial systems, communication infrastructure, and voting processes, to govern society. As these institutions become digitized in the post-internet era, including through the adoption of blockchain technology, then blockchain system design requires deliberate attention regarding the promises of decentralization and "trustless" security that are often assumed.

Governance in blockchain-based systems presents a unique set of security challenges. Governance rules are encoded in the technical aspects of blockchain-based systems and, thus, formalized in software code. The aim of governance in sociotechnical settings is to recognize the need to support flexible interactions among participants in the administration of network settings [3]. While public blockchains encourage people to participate in software development, consensus mechanisms, and ongoing governance decisions, private blockchains maintain these governance functions centrally, reducing the role of people to that of "users," rather than participants. Despite the popularity of blockchains as an infrastructural solution, these contexts of public and private governance matter for those using these systems. A sociotechnical lens to analyze governance in blockchains questions what is external, or "constituted of," and what is internal, or "constituted within," via interactions between administrators, technology, participants, and other stakeholders in the network [19].

More limited security frameworks that only focus on the technical components of a system do not fully address the challenges of participatory information systems, as they tend to disassociate people as "passive recipients of engineering decisions" instead of orienting the system around the expectations and needs of people [20]. This is not to say that existing security practices are unnecessary or wrong, but rather that science and technology studies can further enhance security practices by drawing in an analysis of the social aspects of a system. This is especially relevant in digital systems that operate in an institutional infrastructure role in society, such as blockchain. Systems that are secure when used by people, known as "effective security," are complex and difficult to achieve because of gaps in the designer's awareness of user goals, threats, and behaviors in practice [21].

There are numerous frameworks by which to guide a sociotechnical analysis of blockchains. Rather than inventing a new security framework, this chapter adopts a general sociotechnical security approach and applies this to blockchains as macrosocial institutional technology.

Sociotechnical security offers a general approach to study the interacting layers of technical, social, and contextual aspects of security, by asking "who in the community participating in the network is in need of protection?", "what features can be exploited within this dynamic, human network—including technical as well as agency, governance, and influence?", "what are the external and internal threats to participants, including other participants?", and "who is responsible and accountable for securing participants in the network?" [20]. An example of a specific sociotechnical security framework is "Sociotechnical Attack Analysis" or "STEAL," which supports both a formal technical analysis and a hypothetical deductive social analysis of a complex system [21]. Security threats in sociotechnical systems relate to both intentional and nonintentional exploits. Latour refers to using a system outside of its anticipated context of use or application as "antiprograms," arguing that this can be counter to the designer's intent [22]. These lenses require us to consider the expectations and needs of participants in the system. If blockchains are to be applied as organizational and macrosocial structures, a sociotechnical understanding of blockchain security is required, to place the participants within the system as the referent focus of security.

The "people security" approach takes an existing sociotechnical security framework and applies it to blockchain, to investigate the role of people in both public and private blockchain instantiations. "People security" applies a simple, pre-existing three-layer sociotechnical security analysis to blockchains. This includes the social layer (people and processes), the software layer (code and applications), and the infrastructure layer (physical and technological infrastructure) [8].

The next section of this chapter applies a sociotechnical security analysis to blockchains to address how the social, technical, and infrastructural layers of the system are interconnected, with the aim of revealing assumptions about where and how blockchains are applied in relation to context, participant needs, and expectations. The aim of this approach is to determine if blockchain systems serve the security needs of users and whether the blockchain architecture of private, with people as "users," or public, with people as "participants," makes a difference to their security as a social outcome of the system.

6 People Security and Public Blockchains

Public blockchains remove the ability for central parties to unilaterally change the rules of the system to secure users against third-party interference. They do so by aligning economic incentives among participants to enable "trustless" interactions, whereby actors or "nodes" in a network can collaborate with others they do not know or trust. This is often referred to as "trustlessness" [23]. The notion of blockchains as a trustless technology has been reinforced in numerous studies on blockchains, advocating for "code as law," whereby participants can collaborate with others that they do not know or trust according to the rules of the software code-governed network [24].

Yet, "trustlessness" requires trust. Rather than a rhetoric of trustlessness, we must interrogate who is being trusted to design, deploy, and secure blockchain-based systems against the expectations of participants in that network to afford or undermine security guarantees about user information, user-owned value, and more. Blockchain security as a guarantee against the threat of centralization and a promise of trustlessness can be misleading.

In the first instance, the rules of blockchain-based technology are a product of the context and beliefs in which they were developed and then applied. For example, the narrative of "trustlessness" is heavily embedded in the libertarian ideology and tech-utopian narratives that have informed the development of the technology [18]. The development of peer-to-peer electronic cash emerged from the discourse and action of the "cypherpunks." This heterogeneous group of cryptography advocates, developers, and philosophers jointly participated in an online mailing list, administered by cryptoanarchists Timothy May, Eric Hughes, and John Gilmore [25]. This politics heavily influences the ideology and security aspirations of public blockchains.

In public blockchains, the ideology of trustlessness refers to the "cypherpunk philosophy of leveraging the economic cost of an attack on the network vs. the cost to use and maintain it, to preserve the autonomy of individuals that are reflected in cryptoeconomics consensus mechanisms" [26]. Trustlessness in not requiring third-party verification to execute transactions has been conflated with broader meanings of trust, which can create misleading assumptions regarding the capabilities of blockchains for users beyond the initial context [27]. Bitcoin, the initial "peer-to-peer electronic cash," is described by its inventor, the pseudonymous "Satoshi Nakamoto," as being "an electronic payment system based on cryptographic security instead of trust allowing any two willing parties to transact directly with each other without the need for a trusted third party" [28]. From these origins, trustlessness is a normative property that represents what people *hope to achieve* with blockchain technology, rather than a security guarantee.

Trustlessness really refers to "trust minimization," as it is not possible for participants to maintain zero trust at every layer of the blockchain [29]. When blockchains are applied to manage macrosocial interactions that are responsible for the coordination of, and arbitration between, people in society, they function as institutions. The aim here is not to substitute human trust with computation but to offer trust guarantees through technical and social mechanisms, thus establishing "trustful" infrastructures [30].

Public blockchains require trust between stakeholders in numerous ways. Trust between people is required on an ongoing basis between stakeholders in the "multi-sided" aspects of a blockchain-based system, including code development by developers, maintenance by miners, and participation by users. For example, coordination between software developers is necessary in each change to the software protocol code, such as issuance of a cryptocurrency (e.g., Initial Coin Offering) and network upgrades or "forks" [31]. Similarly, the consensus mechanism that affords the system with "fault tolerance" depends on access to hardware "miners." Satoshi highlighted that it is computationally impractical for an attacker to change the public history of transactions "if honest nodes control a majority of CPU power" [28]. Yet, at the infrastructure layer, cryptocurrency hardware mining has become an extremely competitive industry across the manufacturing and supply chain, where innovation gains in computing power (such as the leap from GPU miners to ASIC miners) can "pre-mine" with increased hash rate to win more cryptocurrency-based block rewards, before releasing the technology to market [32]. According to a study by the University of Cambridge which analyzed the Internet Protocol (IP) addresses of Bitcoin miners, China controls 65% of the mining power or "hash rate," with the United States second at just over 7% [33]. This means that collusion might influence the underlying record of transactions in forks or other governance disputes, thus demonstrating the need for trust in some actors in the network for blockchain security.

Transition from “proof-of-work” to “proof-of-stake” consensus is also a social coordination process. Proof-of-stake is the proposed solution to the risk of centralization of hardware miners in “Ethereum,” the second largest blockchain by market capitalization. Yet, barriers to entry exist in the requirements to own substantial amounts of cryptocurrencies to “stake” in order to validate transactions and secure the blockchain, and this process can be socially engineered. Cryptocurrency “whales” who own enough funds to move the market (such as initial team members of a project or hedge funds) can collude to dominate the staking market or “flash-crash” the market price of a cryptocurrency to endanger the security of the protocol. Another vulnerability of staking-based public blockchains is that trust can be allocated to “staking pool” infrastructure providers. These “staking-as-a-service” providers set up and maintain validator nodes for large proportions of some protocols, which forms points of failure if their systems or processes are compromised [34]. In reality, blockchain technology can be compromised at the technical, software code, and social coordination layers in systems that are shaped by software engineers, social processes, and market forces.

Another limitation to “trustlessness” in public blockchain security is that the social layer of governance is still in open experimentation and is not yet, if at all, decentralized. This includes the invention of software-based governance via “decentralized autonomous corporations” (DACs), later termed “decentralized autonomous organizations” (DAOs) [35]. The idea is not to replace trust with code but to provide accountability by making the rules of the system transparent through publicly available, open-source code [36]. Yet, decentralized infrastructure does not necessarily lead to the decentralization of influence within that infrastructure. “Any blockchain-based organization whose governance system relies mainly or exclusively on market dynamics is, therefore, ultimately bound to fail” [37]. Despite technical sophistication, security through decentralization and trustlessness at the micro and meso levels in public blockchains is difficult to achieve due to social, technical, and infrastructural dependencies.

6.1 Decentralized Autonomous Organizations

Public blockchains are most readily being adopted as the infrastructural base for decentralized autonomous organizations (DAOs). The fundamentals of “Decentralized Autonomous Organizations” (DAOs) are a community of participants, working toward a shared objective that leverage decentralized technologies to do so in a scalable manner. The term DAO emerged out of the field of cybernetics to describe a multi-agent system that self-governs toward an objective [38]. DAOs have been defined in relations to blockchain communities as “a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralised (i.e. independent from central control)" [39]. DAOs are heterogeneous, meaning that the goals, scale, and participants of DAOs vary widely. They can be micro- or macro-scale, be socially focused or technologically focused, and exist for purposes such as shared investment vehicles, special interest hobby groups, or software development (e.g., Flamingo DAO, Seed Club, and 1Hive). There have been rapid uptake and prolific growth of the number, size, and purposes of DAOs since the term was adopted in blockchain communities in 2015 [40].

DAOs enable people to participate in the ownership and governance of coordination infrastructure. For example, "ConstitutionDAO" was a group of people that collectively pooled funds in a failed attempt to purchase an original copy of the US Constitution [41]. This has led to ongoing social experimentation in self-governance and collective action. People also initiated a number of funding DAOs to rapidly raise millions of dollars to donate to support others in the crisis in Ukraine [42]. Due to their flexibility and scalability, DAOs may be the avenue for more widespread adoption of public, permissionless blockchain infrastructure.

The next section explores a number of private blockchain case studies by applying the sociotechnical people security framework to investigate the social, software, and infrastructure layers of private blockchains in action at a macrosocial level, including which community participating in the network is in need of protection, what features can be exploited within the network, and who is responsible and accountable for securing participants in the network. In contrast to public blockchains, permissioned blockchains are more readily being applied to macrosocial uses at a societal level on communities outside of software developers themselves, and thus this context has been chosen for the analysis of private blockchains as relevant to assess against the parameters of the sociotechnical "people security" approach.

7 Applying a Sociotechnical Security Analysis to Private Blockchain Networks

Private blockchains are prevalent in a number of real-world, macrosocial-level applications across humanitarian, government, and corporate applications. Each case study below focuses on a use case of blockchain as a macrosocial institutional infrastructure for coordinating goods, services, and people in society. Each example is then run through a sociotechnical analysis.

7.1 Humanitarian Case Study: Blockchain-Based Cash Voucher Assistance

Blockchains have been piloted in a number of humanitarian, not-for-profit organization use cases at the macrosocial level, predicated on governing the most vulnerable with efficiency. While some "humanitarian"-oriented adoption is localized and organic, in response to hyperinflation and mistrust in government, like that of Venezuela, many cases are centrally issued by not-for-profit or aid organizations [43].

One of the first high-profile humanitarian use cases of blockchain is the World Food Programme's (WFP) "Building Blocks" project [44]. Blockchains were applied in the project as a ledger of transactions and settlement layer to transfer cash aid to Syrian refugees in a Jordanian refugee camp. The system is intended to "create more choice" for refugees to spend their cash aid at the supermarket [44]. The project received overwhelmingly positive coverage in the media [45]. However, this blockchain-based system has a number of shortcomings which could equate to significant people security vulnerabilities for participants.

The community participating in the network in need of protection are Syrian refugees, who are a highly vulnerable population fleeing a civil war. Protection of identity is a necessity for this population [46]. Yet, digital identities are being created that are permanently linked to biometric indicators which could then be hacked and traced back to family members or used as leverage to direct behaviors. Biometric registrations were made mandatory when receiving cash aid, making participation in the system mandatory and not voluntary.

Furthermore, a number of technical and social features can be exploited in the system. The system is inextricably linked in political and infrastructural contexts which may not be in the best interests of users. For example, the blockchain is centrally issued and administered by WFP, and administrative access is afforded to a consortium of international aid organizations [47]. This results in significant power asymmetries in terms of how the system operates, what data is recorded, where it is stored, who has permission to access the data, and for what purposes. The biometric iris scanners used are provided by a local Jordanian company, IrisGuard, meaning persistent, biometric digital identities of refugees are being stored locally. The UN Refugee Agency (UNHCR) has also used IrisGuard to register and store the irises of 2.5 million people on UNHCR's "Eyecloud" server, alongside other personal data for cross-referencing [48]. Once data is recorded, it is hackable, replicable, and vulnerable to technical or human exploitation [49]. The IrisGuard database and Eyecloud are also linked to Amman Bank ATMs in Jordan, where refugees can scan their eyes and withdraw cash. Numerous technical systems and levels of cybersecurity, as well as numerous permissions to access and correlate highly sensitive data, with little to no consent from participants persist throughout this system.

In this case, accountability falls on the humanitarian agencies who are responsible for ethically providing aid without establishing systemic vulnerabilities for recipients. Although the system may provide operational control and coordination efficiencies among aid agencies, this instantiation of the digital economy inextricably links the biometric digital identity of refugees with an immutable ledger, across numerous local and international databases. This means that the system is not cryptographically secure and requires significant trust in the IT security of local companies and government agencies. Here, blockchain is simply a database which is centrally issued and administered, rather than a digital infrastructure that empowers users to participate in the ownership or governance of the system.

Similar private, blockchain-based applications in humanitarian contexts are being explored by UNICEF, the Human Rights Foundation, the International Federation of Red Cross, and Oxfam [50].

7.2 Government Case Study: Central Bank Digital Currencies

Blockchains are also gaining prominence as the infrastructure for nation-state central bank digital currencies (CBDCs). The development of national CBDCs is underway in multiple countries, including Australia, Canada, and China [51]. Public blockchain platforms that enable digital currency, such as Bitcoin and Facebook’s “Libra” platform, are perceived as competitors to nation-state central bank-issued currency in the move for governments to issue their own central bank digital currency [52]. Some of the justifications for CBDCs include financial inclusion of people in remote and marginalized regions and consumer protection as a low-cost interbank settlement layer. However, what Canada has coined the “road to digital currency” has been referred to in the case of China as “the road to digital unfreedom,” with fears of state surveillance, as the system is designed in the interests of administrators, with centralized development, issuance, and governance [53].

Digitization of entire nation-state monetary systems creates astounding data security vulnerabilities for populations. Significant concerns have been raised on the data security of government-led databases, as this sensitive national data creates a target for hackers from both the inside and the outside that could be exploited for geopolitical reasons [54].

Unlike other digital asset platforms, CBDCs may not be voluntary for participants. As digital identity, value, and transactions are tied to citizenship, participation in CBDCs could be mandatory. The system is not intended to be decentralized or interoperable in order to circumvent the threat of centralization.

Furthermore, the myth of financial inclusion is predicated on access to proprietary computing devices and digital literacy, most of which is not within reach of the most vulnerable, who rely on the cash economy [55]. The aims of CBDCs are antithetical to the public blockchain ideology of decentralization. CBDCs will not offer anonymity, and the advantages of cash for users to avoid exposure to customer profiling or hacking will be lost in the transition to digital currency.

Of course, CBDCs are contextual, and the risks differ according to where and how the system is designed and issued [56]. In general, the introduction of CDBCs could lead to disintermediation of the banking sector, trigger digital bank runs, and threaten banks' liquidity and business models [57]. Given the risks to participants in the network vs. the gains, CBDCs do not offer a positive macrosocial infrastructure that is private, decentralized, censorship resistant, or cost-saving and places a significant burden on the state to secure technical infrastructure and the data of citizens against geopolitical threats.

7.3 Corporate Case Study: Private Currency Platforms

Corporations are also able to leverage their user audience to issue blockchain-based platforms. In corporate situations, blockchains are often applied internally, to perform a specific function in corporations and industry, such as transparent record keeping, as a tool for organizational efficiency, and cost reduction [58]. Here, blockchains are often private or permissioned networks, responsible for coordination of supply chain goods and record keeping between known, distributed parties. Examples include supply chain experimentation to ship and trace almonds from Australia to Germany and J.P. Morgan's "JPM Coin" for interbank settlement between institutional clients [59]. However, corporate blockchain-based currency platforms have also been proposed, such as the prominent case of Facebook's "Libra" blockchain (now re-branded to "Diem").

Facebook's Libra blockchain was proposed as a solution for global payments and financial inclusion. Through its own digital wallet called "Calibra," Facebook is aiming to capture the "super-app" trend by forming a digital ecosystem within its own services to capture customers. China has already digitized the majority of consumer payments through corporate giants Alibaba and Tencent "digital wallet" applications which account for 90 percent of the $17 trillion mobile payments' market in China in 2017 [60]. Due to Facebook's poor record on consumer protection and user privacy, alarms were raised by global data protection and privacy enforcement authorities [61]. Libra raises significant concerns regarding the security of participants in the network.

When they made this announcement, Libra was heavily criticized as competing against sovereign currencies and because of Facebook's record of consumer protection and privacy breaches. A number of "Libra Association" consortium members subsequently left, including PayPal, eBay, Mastercard, Stripe, and Visa [62]. A top Senate Banking Committee official stated that "we cannot allow giant companies to assert their power over critical public infrastructure. The largest banks and the largest tech companies do not act in the interest of working Americans, but in the interest of themselves and their investors" [63]. This instantiation of privately owned and governed blockchain as a potentially global payment railway became a critical public infrastructure in society. Thus, security for users is paramount and yet it is lacking.

The revised Libra 2.0 promotes itself as secure, "built on blockchain technology and designed with security in mind" [64]. Yet, it is not technically, socially, or infrastructurally robust against exploitation; governing members that buy-in to the Libra Association are responsible for validating transactions on the network (noting that this may be transitioned in the latter proposed version of Libra). While the privacy of participants was said to match that of existing cryptocurrencies, access to personally identifiable information via the Libra "digital wallet" (the local user interface that sends and receives transactions) has not been specified and may be accessible by Facebook and its affiliates. Libra, now Diem, was set to launch in 2022 and make a significant impact on the payments sector and the business modes of banks by offering a cheaper mean of cross-border remittance for consumers. Yet, having struggled to convince regulators that Facebook should administer a global digital currency, the company announced that the project was winding down for good in January [65]. It was mistrust in the operator that led to its failure to launch.

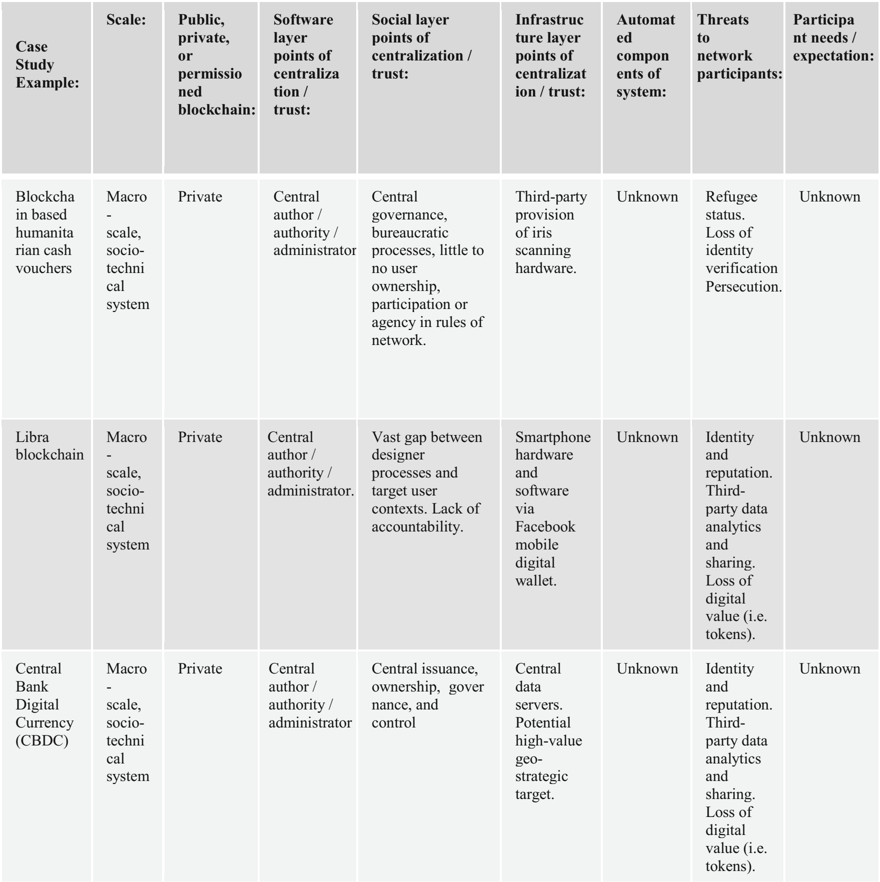
The broader implications of this lack of accountability or recourse for the security of users' digital information and assets remain opaque.

8 Observations and Findings

The trust and security guarantees of blockchains depend on the type of blockchain, the context in which it is applied, and the needs of participants. Blockchain security is dependent on how social and technical aspects of the system interact, the threat which participants believe they are optimizing against by using the system, who is trusted to fulfil certain functions in the system, and why a blockchain is being applied. Empirical analysis via desktop-based research and case study investigations of the application of both public and private blockchains demonstrate that blockchains are fraught with security assumptions and shortcomings on the promise of system issuers toward system users at the social, software, and infrastructural levels.

There is a major discrepancy between the promise of "security," "decentralization," and "trustlessness" embedded in the origins of public blockchains and attribute of encryption and the real threats, needs, and expectations of users in the contexts that blockchains are being applied by centralized authorities. In private blockchains, security via decentralization is not an objective, as they are centrally administered by design and users do not have a participatory role in system design or governance.

Yet, each private blockchain case study also reveals serious contextual gaps about the advantages of using a blockchain for the application and the security context and needs of the users of those systems. Private blockchain architecture is most commonly being adopted in macrosocial contexts, where a public blockchain may be more suitable to afford privacy and security guarantees to users. In each private blockchain case described, threats are initiated and experienced by a number of stakeholders across the different technical and governance layers of the blockchain



Case Study Example:	**Scale:**	**Public, private, or permissioned blockchain:**	**Software layer points of centralization / trust:**	**Social layer points of centralization / trust:**	**Infrastructure layer points of centralization / trust:**	**Automated components of system:**	**Threats to network participants:**	**Participant needs / expectation:**
Blockchain based humanitarian cash vouchers	Macro-scale, socio-technical system	Private	Central author / authority / administrator	Central governance, bureaucratic processes, little to no user ownership, participation or agency in rules of network.	Third-party provision of iris scanning hardware.	Unknown	Refugee status. Loss of identity verification Persecution.	Unknown
Libra blockchain	Macro-scale, socio-technical system	Private	Central author / authority / administrator.	Vast gap between designer processes and target user contexts. Lack of accountability.	Smartphone hardware and software via Facebook mobile digital wallet.	Unknown	Identity and reputation. Third-party data analytics and sharing. Loss of digital value (i.e. tokens).	Unknown
Central Bank Digital Currency (CBDC)	Macro-scale, socio-technical system	Private	Central author / authority / administrator	Central issuance, ownership, governance, and control	Central data servers. Potential high-value geo-strategic target.	Unknown	Identity and reputation. Third-party data analytics and sharing. Loss of digital value (i.e. tokens).	Unknown

Fig. 1 A ‘people security’ analysis of various blockchain architectures

network with little accountability for the issuers who are responsible for designing, deploying, owning, or governing the system. This is both an information asymmetry and a misalignment of incentives between system administrators and users.

From these findings of the shortcomings of blockchain applications as a sociotechnical solution, the following table can be drawn as a simple tool for the analysis of people security in blockchains. This framework was adapted from Goerzen et al.’s sociotechnical security framework analysis, which has been applied to social media systems [20], and Li et al.’s security requirements analysis for sociotechnical systems [8] (Fig. 1).

8.1 Trust, But Verify: Applications and Limitations of the "People Security" Model

Buterin defines trust as "assumptions about the behavior of others," of which one dimension of failure is how badly the system would fail if this assumption is not met [66]. The security concern about a misalignment of assumptions between system designer and user is "how badly will the system fail if the security assumption of the user is violated?". In the cases outlined above, the results of a system failure, such as leaked identity or loss of one's personal digital assets and the value they represent, could be severely damaging to the referent user of community in need of security within the system. This analysis outlines technical and social security limitations in both public and private blockchains, as well as considers the context in which blockchain is applied and the participants in the system. When users are not entitled to participate in the ownership and governance of the system, their security can more easily be compromised.

In public blockchains, the role of people in participating in the network is threefold. People are invited to participate in developing the open-source code of the network, people are needed to secure the network by validating transactions and maintaining their software through the consensus mechanism of mining in proof-of-work or staking in proof-of-stake, and people are able to govern the network by participating in community discussions, voicing proposals, and voting on movements. Although not completely "decentralized," "trustless," or secure, user participation in the function and governance of the network enables new types of macrosocial institutional digital infrastructure, in which sociotechnical security is a consideration.

In contrast, private and permissioned blockchains in social coordination contexts position people as "users," with less agency, authority, or transparency over how the system functions compared to those responsible for designing, issuing, and administrating the system. There is little to no role for participation in developing, securing, or governing the network. This limits the ability of private blockchains to offer people security to users of the system through the unique cryptoeconomic attributes evident in public blockchains of decentralization and trust minimization.

Private blockchains are being applied by private institutions and government bodies. Meanwhile, public blockchains are being adopted for community initiatives that demand self-organization, initially in the software developer communities in which they are created but now more broadly. As applications and adoption broaden, the distinctions and differences in security affordances for different blockchain architectures are imperative for the literacy of those using them. Experimentation with public blockchains and "Decentralized Autonomous Organizations" across different applications may be a suitable area for further exploration of sociotechnical security research.

8.2 *In Code We Trust? The Limitations of Security in Blockchains*

Blockchains are a sociotechnical construct, and as such, blockchain security is not only about network security; rather, we must also consider participants in the network as owners, operators, and/or users. Both public and private blockchains possess sociotechnical security vulnerabilities at the social, software, and infrastructure layers. Citizens of public blockchain-based macrosocial digital institutions are warned: “there is no proven linear-causal relationship between decentralization in technical systems and equitable practices socially, politically or economically” [67]. There is, however, a transition of trust from existing institutions toward the designers and governors of public blockchain infrastructure.

Meanwhile, private and semi-permissioned blockchain-based systems are similar to many other web-based technologies. They are invisible infrastructures which operate behind user interfaces and often without legibility to users [68]. This means that unless the software code that governs the system is open-source *and* participants know how to audit (or read) code, they do not know how it has been designed to work. Thus, many applications of blockchain systems in the real world are permissioned and oftentimes typify the threat of centralization by codifying dependence on private actors.

At the software level, blockchain security can be compromised by vulnerabilities in the code itself. Examples include privacy limitations through upgrades to the core cryptographic primitives, traceability and monitoring of pseudonymous public key addresses, network monitoring through traffic analysis, and increasingly sophisticated blockchain analytics services which deanonymize actors in the network [69]. Furthermore, people’s digital assets are also vulnerable through shortcomings in blockchain code, such as the infamous “DAO” hack in which around $60 million (at the time) was stolen from a “decentralized, automated” smart contract which allowed for double withdrawals because a single line of code was not in the correct order [70]. The pursuit of decentralization also places significant onus on people to manage their own “private keys,” or cryptographic passwords, through secure storage [71]. A number of other crucial technical issues remain unresolved in the proposal for the latest version of Ethereum at the time of writing, which is predicted to become the largest public blockchain by market capitalization and users upon launch.

At the social level, social processes continue to enable and restrict both public and private blockchain applications. Regulation remains an ongoing ambiguity for participants in blockchain systems. As a “polycentric enterprise” comprised of participants, network validators, and exchanges, public blockchains are subject to a variety of governance restrictions, depending on jurisdiction [72]. Shortcomings also exist in the asymmetries in the surrounding context of how and where blockchains are deployed. Most cryptocurrency Initial Coin Offerings (ICOs) project launches have come out of the United States, but people from around the world invest at their own risk, with little to no legal recourse in the event of loss. The

Library Law of Congress notes that one of the most common government responses to cryptocurrency is to issue warnings about investing. "Such warnings, mostly issued by central banks, are largely designed to educate the citizenry about the difference between actual currencies, which are issued and guaranteed by the state, and cryptocurrencies, which are not" [73]. ICOs have been regulated in numerous countries due to the risk to retail investors of investing in volatile assets with no stable underlying value—highlighting digital illiteracy in establishing realistic expectations of what blockchain is and does.

In terms of governance, centralization exists at multiple intersections in blockchain-based infrastructures. In private blockchains, issuance and administration of blockchain-based networks are often synonymous with network ownership and control. In public blockchain, early espoused ideologies of blockchain being decentralized to create freedom and choice for individuals created security assumptions for participants. Yet, tokens are often owned by a concentration of actors and software and governance decisions are often made by a small group of people.

At the infrastructure layer, significant security issues exist in the hardware and infrastructure dependencies of blockchains. This includes reliable internet connectivity, which forms the basis of the underlying infrastructure which blockchain networks are dependent upon. Although much development was funded by the Defense Advanced Research Projects Agency (DARPA), the internet began with a vision of creating a "decentralized commons" that was coopted by private and commercial interests [74]. Yet, the centralization of information, ownership, and influence on the internet reveals significant limitations in the assumption that the blockchain digital economy can be decentralized, because it is dependent on the existing infrastructure of the internet. The same is true of hardware dependencies, such as mobile phones and computer hardware.

8.3 Blockchain Evolution and Security Concerns: Looking Ahead

As blockchain holds a potentially significant trajectory in critical economic and governance infrastructure in society, "people security" offers a critical lens for both designers and users for transparent, voluntary participation in systems that clarify design assumptions and the context in which they are applied.

Pursuing people security could also help to reveal design assumptions and user needs as functions within blockchain-based systems become more automated. "Because artificial intelligence is about the automation of cognitive processes, and blockchain is the automation of transactions, there are specific scenarios where both technologies can be combined. A blockchain network can provide a decentralized platform to support some advanced AI capabilities" [75]. Automation of certain rules and functions by combining them with other emerging technologies such as artificial intelligence (AI) has the potential to semi-autonomously govern interactions based on how the system is encoded through smart contracts, DAOs, and machines—thus lessening the agency of participants [76]. Suggested use cases for automated blockchains include data marketplaces, explainable AI, and the Internet of Things (IoT) [77].

While blockchains may enable *more* decentralized instantiations of AI, the *assumption* is that this is decentralized and therefore secure, without always considering those assumptions apply to the human participants in the network. In such cases, trust is reallocated from existing institutions to semi-autonomous digital agents to act on behalf of people, weakening the barrier between the rules of the digital world and the physical world, yet software code is subjective and reflects assumptions about behavior in the real world that are contained in theoretical models of the system designer [78]. Therefore, surfacing where and how automation is occurring in a system through transparent code is a crucial first step to minimizing complexity to apply a people security approach. Further analysis is required into the effects of automation in blockchain systems on people security.

In some circumstances, blockchains may not be a desirable macrosocial infrastructure to afford security to people at all, due to the fundamental assumptions that shape the attributes of blockchain-based systems. Some of the values that blockchains institute, such as immutable records of data, have the potential to conflict with privacy, legal frameworks, and data norms. Other peer-to-peer protocols offer a different ontology which is not based on rational, economic self-interest and individualism. By contrast, the Holochain team encourages a "post-blockchain," "agent-centric," cryptographically secure data infrastructure which does not require digital tokens for data sharing, access, storage, and verification of public data [79]. Similarly, Dat protocol offers data hosting through an "append-only" protocol that runs on a distributed, peer-to-peer network of computers that can work offline or with poor connectivity, whereby the original uploader can add or modify data while keeping a full record of history and cryptographic keys are often shared for collective governance of digital assets [80]. The fundamental assumptions of decentralization, trustlessness, immutability, and security that undergird blockchain systems must be made explicit in order to assess the suitability of the protocol by potential users and carefully consider the needs, trade-offs, and consequences for participants.

9 Conclusion and Further Directions

As a tool, blockchains possess unique, cryptoeconomic properties that are useful for some applications. As an organizational infrastructure, blockchains enable some decentralization by reallocating trust to other parties. Blockchains are a macrosocial coordinating technology in society, with interlinked technical and social functions, including automation, oracles, smart contracts, voting, and digital currency. When applied to macrosocial coordination problems, it is imperative to analyze blockchain security as "people security" to more accurately assess the type of blockchain and the context of the application against the social, software, and infrastructure requirements of participants using the system. If blockchains are to be applied as institutions, we need the best institutions possible for society.

There are no blanket security guarantees afforded by blockchains. Blockchain technology possesses different attributes and varying levels of security for people participating in a system, depending on the design decisions, issuance, administration, and context in which it is applied. Many security assumptions of blockchain are embedded in the political ideologies from which the technology emerged, rather than the test cases that are being deployed by companies and governments. This research chapter has found that there are a number of security and trust issues that need to be addressed in both public and private blockchains, especially as centralized, private blockchains which limit the autonomy of users are most commonly being employed in macrosocial contexts. In uncovering the assumptions regarding the promises and expectations of both public and private blockchains, it is clear that blockchain security, in its current form, has significant security limitations for people as participants in this infrastructure.

While blockchain-based networks are distributed, users must understand that both public and private blockchains are far from decentralized. This sociotechnical analysis of "blockchain security" as "people security" can support system designers and participants to clarify expectations, assumptions, and guarantees when deploying and employing these tools as systems in order to acknowledge user expectations and communicate realistic security guarantees.

This research leads to a number of further directions for investigation. This includes the application of the people security framework to different use cases for deeper sociotechnical security analysis of specific blockchain implementations and user groups, further comparability of different blockchain designs to analyze the people security trade-offs implementations, and investigation into the social outcomes of automated processes within blockchain-based systems.

References

1. S. Singh, N. Singh, Blockchain: Future of financial and cyber security, in *2016 nd International Conference on Contemporary Computing and Informatics IC3I*, (2016), pp. 463–467. https://doi.org/10.1109/IC3I.2016.7918009. S. Underwood, Blockchain beyond bitcoin. Commun. ACM. **59**(11), 15–17 (2016). https://doi.org/10.1145/2994581
2. A. Shahaab, R. Maude, C. Hewage, I. Khan, Blockchain: A panacea for trust challenges in public services? A socio-technical perspective. J. Br. Blockchain Assoc **3**(2), 6 (2020). https://doi.org/10.31585/jbba-3-2-6. Available at: https://www.researchgate.net/publication/343307094_Blockchain_A_Panacea_for_Trust_Challenges_In_Public_Services_A_Socio-technical_Perspective. Accessed 30 Nov 2020
3. M.P. Singh, Governing sociotechnical systems, in *2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, (2011), p. 1. https://doi.org/10.1109/WI-IAT.2011.288

4. E. L. Trist, The evolution of socio-technical systems: a conceptual framework and an action research program. Occasional Paper No. 2, Toronto, ON, Canada: Ontario Quality of Working Life Centre (1981)
5. S. Voshmgir, M. Zargham, Foundations of cryptoeconomic systems, in *Cryptoeconomics Working Paper Series*, (Vienna University of Economics, 2019), p. 1
6. A. Hayes, The socio-technological lives of bitcoin. Theor. Cult. Soc. **36**(4), 49–72 (2019). https://doi.org/10.1177/0263276419826218
7. W.E. Bijker, T.P. Hughes, T. Pinch, *The Social Construction of Technological Systems*, Anniversary edn. (The MIT Press, Cambridge, MA, 2012) Available at: https://mitpress.mit.edu/books/social-construction-technological-systems-anniversary-edition. Accessed 07 Aug 2020
8. T. Li, J. Horkoff, J. Mylopoulos, Holistic security requirements analysis for socio-technical systems. Software Syst. Model. **17**, 1253–1285 (2018). https://doi.org/10.1007/s10270-016-0560-y
9. C. Berg, S. Davidson, J. Potts, Blockchain technology as economic infrastructure: Revisiting the electronic markets hypothesis. Front. Blockchain. **2** (2019). https://doi.org/10.3389/fbloc.2019.00022
10. V. Buterin, *The Meaning of Decentralization* (Medium (blog), 2017) Available at: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Accessed 12 June 2020
11. K. Nabben. (2021). *Imagining Human-Machine Futures: Blockchain-Based 'Decentralized Autonomous Organizations'*. Available online: https://ssrn.com/abstract=3953623. Accessed 1 Mar 2022
12. L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, S. Shimizu, *Privacy Preservation in Permissionless Blockchain: A Survey* (Networks, Digital Commun, 2020). https://doi.org/10.1016/j.dcan.2020.05.008
13. G.O. Karame, E. Androulaki, *Bitcoin and Blockchain Security* (Artech House, Norwood, MA, 2016) X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems. Future Generat. Comput. Syst. **107**, 841–853 (2020). https://doi.org/10.1016/j.future.2017.08.020
14. I.C. Lin, T.C. Liao, A survey of blockchain security issues and challenges. Int. J. Netw. Secur., 19–15 (2017). https://doi.org/10.6633/IJNS.201709.19(5).01. H. Chen, M. Pendleton, L. Njilla, S. Xu, A survey on Ethereum systems security: vulnerabilities, attacks and defenses (2019). Available at: http://arxiv.org/abs/1908.04507. Accessed 08 Aug 2020; R. Zhang, R. Xue, L. Liu, Security and privacy on blockchain, ArXiv190307602 Cs (2019). Available at: http://arxiv.org/abs/1903.07602. Accessed 08 Aug 2020
15. D.W.E. Allen, A. Lane, M. Poblet, The governance of blockchain dispute resolution. Social Sci. Res. Netw. (2019). https://doi.org/10.2139/ssrn.3334674
16. C. Berg, S. Davidson, J. Potts, *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics* (Edward Elgar Publishing, Ottawa, 2019)
17. L.M. Bach, B. Mihaljevic, M. Zagar, Comparative analysis of blockchain consensus algorithms, in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, (2018), pp. 1545–1550. https://doi.org/10.23919/MIPRO.2018.8400278
18. T. C. May, Cyphernomicon (1994). Available at: https://web.archive.org/web/20110607130638/http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html. Accessed 15 Aug 2020
19. A. Smith, A. Stirling, Moving inside or outside? Positioning the governance of sociotechnical systems, *Science and Technology Policy Research, SPRU electronic working paper series*, Brighton: University of Sussex. Paper No. 148 (2006)
20. M. Goerzen, E.A. Watkins, G. Lim, Entanglements and exploits: Sociotechnical security as an analytic framework, in *9th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 19)*, (2019)

21. A. Ferreira, J.L. Huynen, V. Koenig, G. Lenzini, A conceptual framework to study sociotechnical security, in *Human Aspects of Information Security, Privacy, and Trust*, (Cham, 2014), pp. 318–329. https://doi.org/10.1007/978-3-319-07620-1_28
22. B. Latour, Technology is society made durable. Sociol. Rev. **38**(S1), 103–131 (1990). https://doi.org/10.1111/j.1467-954x.1990.tb03350.x
23. Y. Xinyi, Z. Yi, Y. He, Technical characteristics and model of blockchain, in *2018 10th International Conference on Communication Software and Networks (ICCSN)*, (2018), pp. 562–566. https://doi.org/10.1109/ICCSN.2018.8488289
24. G. Vidan, V. Lehdonvirta, Mine the gap: Bitcoin and the maintenance of trustlessness. New Media Soc. **21**(1), 42–59 (2019). https://doi.org/10.1177/1461444818786220
25. T. C. May, The crypto anarchist manifesto (1992). Available at: https://www.activism.net/cypherpunk/crypto-anarchy.html. Accessed 15 Aug 2020; E. Hughes, A Cypherpunk’s Manifesto. in *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance* (Wiley (1997), (1993)), pp. 285–87
26. V. Buterin, *A Proof of Stake Design Philosophy, Medium* (2016). Available at: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51. Accessed 16 Aug 2020
27. U.W. Chohan, Are cryptocurrencies truly trustless? in *Cryptofinance and Mechanisms of Exchange: The Making of Virtual Currency*, ed. by S. Goutte, K. Guesmi, S. Saadi, (Springer International Publishing, Cham, 2019), pp. 77–89
28. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2009). Available at: https://bitcoin.org/bitcoin.pdf. Accessed 1 Feb 2020
29. N. Szabo, Money, blockchains, and social scalability. Unenumerated (blog) (2017). Available online: https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html. Accessed 2 Mar 2022
30. K. Nabben, Trustless approaches to digital infrastructure in the crisis of COVID-19 Australia’s newest COVID app. Home-grown surveillance technologies and what to do about it. Soc. Sci. Res. Netw. Rochester, NY (2020). https://doi.org/10.2139/ssrn.3579220SSRN. Scholarly Paper ID 3579220
31. P. De Filippi, B. Loveluck, The invisible politics of Bitcoin: Governance crisis of a decentralized infrastructure. Social Sci. Res. Netw. **5**(4) (2016). https://doi.org/10.14763/2016.3.427
32. K. Grobys, N. Sapkota, Predicting cryptocurrency defaults. Appl. Econ. **52**, 5060–5076 (2020). https://doi.org/10.1080/00036846.2020.1752903. Bitcoinera, Are we decentralized yet? (2018). Available at: https://bitcoinera.app/arewedecentralizedyet/. Accessed 15 Aug 2020; Etherscan, n. d., *Top 25 Miners by Blocks. Etherscan, Ethereum (ETH) Blockchain Explorer* (2021). Available at: http://etherscan.io/stat/miner?range=7&blocktype=blocks. Accessed 15 Aug 2020
33. Cambridge Bitcoin Electricity Consumption Index, Cambridge bitcoin electricity consumption Index (CBECI) (2021). Available at: https://cbeci.org/mining_map. Accessed 16 Aug 2020
34. L.W. Cong, Z. He, J. Li, Decentralized mining in centralized pools. Rev. Financ. Stud. (2020). https://doi.org/10.1093/rfs/hhaa040
35. Ethereum Foundation, DAOs, DACs, DAs and more: an incomplete terminology guide (2014). Available at: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/. Accessed 08 Aug 2020; Y.Y. Hsieh, J.P. Vergne, P. Anderson, K. Lakhani, M. Reitzig, Bitcoin and the rise of decentralized autonomous organizations. J. Org. Des.. **7**(1), 14 (2018). https://doi.org/10.1186/s41469-018-0038-1; A. Wright. The rise of decentralized autonomous organizations: Opportunities and challenges. Stanf. J. Blockchain Law Policy (2021). https://stanford-jblp.pubpub.org/pub/rise-of-daos/release/1
36. P. De Filippi, M. Mannan, W. Reijers, Blockchain as a confidence machine: The problem of trust and challenges of governance. Technol. Soc. **62**, 101284 (2020). https://doi.org/10.1016/j.techsoc.2020.101284
37. P. De Filippi., Blockchain technology and decentralized governance: the pitfalls of a trustless dream (2019). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524352. Accessed 08 July 2020. doi:https://doi.org/10.2139/ssrn.3524352

38. W. Dilger, Decentralized autonomous organization of the intelligent home according to the principle of the immune system. 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation **1**, 351–356 (1997). https://doi.org/10.1109/ICSMC.1997.625775
39. S. Hassan, P. De Filippi, Decentralized autonomous organization. Int. Policy Rev. **10**(2) (2021). https://doi.org/10.14763/2021.2.1556. https://policyreview.info/glossary/DAO
40. Y. Faqir-Rhazoui, J.A. Gallardo, S. Hassan, A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. J. Int. Serv. Appl. **12**, 9 (2021). https://doi.org/10.1186/s13174-021-00139-6. DeepDAO, DeepDAO (n.d.). Available online: deepdao.io/. Accessed 8 Nov 2021
41. A. Brown, Crypto investors lose out in $43.2 million sale of rare copy Of U.S. constitution. *Forbes* (2021). https://www.forbes.com/sites/abrambrown/2021/11/18/constitution-dao-crypto-ether-constitutional-sothebys-sale-auction/?sh=54efaeb66ad4. Accessed 10 Mar 2022
42. W. Gottsengen, New DAO raises $3M in ETH for Ukrainian Army. *CoinDesk* (2022). Available online: https://www.coindesk.com/tech/2022/02/27/new-dao-raises-3-million-in-eth-for-ukrainian-army/. Accessed 10 Mar 2022
43. A. F. Cifuentes, Bitcoin in troubled economies: the potential of cryptocurrencies in Argentina and Venezuela. Lat. Am. Law Rev. 99–116 (2019). https://doi.org/10.29263/lar03.2019.05; A. Kliber, P. Marszałek, I. Musiałkowska, K. Świerczyńska, Bitcoin: safe haven, hedge or diversifier? Perception of bitcoin in the context of a country's economic situation—a stochastic volatility approach. Phys. Stat. Mech. Appl. **524**, 246–257 (2019). doi:https://doi.org/10.1016/j.physa.2019.04.145
44. World Food Programme, Building blocks | WFP innovation (2020). Available at: https://innovation.wfp.org/project/building-blocks. Accessed 08 Aug 2020
45. R. Juskalian, Inside the Jordan refugee camp that runs on blockchain, *MIT Technology Review* (2018). Available at: https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/. Accessed 14 Aug 2020; P. Apte, How blockchain is bringing Food security to refugees, dell technologies (2019). Available at: https://www.delltechnologies.com/en-us/perspectives/how-blockchain-is-bringing-food-security-to-refugees/. Accessed 14 Aug 2020; F. Awan and S. Nunhick, Governing blocks: building interagency consensus to coordinate humanitarian aid. J. Sci. Policy Gov. **16**(2) (2020). https://doi.org/10.38126/jspg160201
46. M. Gillespie, S. Osseiran, M. Cheesman, Syrian refugees and the digital passage to europe: Smartphone infrastructures and affordances. Soc. Media Soc. **4**(1), 205630511876444 (2018). https://doi.org/10.1177/2056305118764440
47. B. Baah, Humanitarian cash and voucher assistance in Jordan: a gateway to mobile financial services (2020). Available at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/01/Jordan_Mobile_Money_CVA_Case_Study_Web_Spreads.pdf. Accessed 14 Aug 2020
48. R. Zambrano, A. Young, S. Verhulst, Case study: connecting refugees to aid through blockchain enabled ID management: world Food Programme's building blocks (2018). Available at: https://www.irisguard.com/media/laglvgzk/building-blocks-case-study.pdf. Accessed 13 Aug 2020
49. Verizon, 2020 data breach investigations report, Verizon Enterprise (2020). Available at: https://enterprise.verizon.com/resources/reports/dbir/. Accessed 15 Aug 2020
50. UNICEF Office of Innovation, UNICEF funding opportunity for blockchain startups (2020). Available at: https://www.unicef.org/innovation/applyBlockchainCrypto. Accessed 08 Aug 2020; L. Cuen, Human rights foundation funds bitcoin privacy tools despite 'Coin Mixing' Legal Stigma, Coin Desk, New York, [Online] (2020). Available at: http://www.coindesk.com/human-rights-foundation-bitcoin-privacy-tools-developer-fund. Accessed Jan 2021; International Federation of the Red Cross (IFRC) Innovation, IFRC blockchain application wins global islamic finance competition. IFRC Innovation (2018). Available at: http://media.ifrc.org/innovation/2018/02/12/ifrc-blockchain-application-wins-global-islamic-finance-competition/. Accessed 08 Aug 2020; ConsenSys, Blockchain for NGOs:

project unblocked cash case study, ConsenSys (2019). Available at: https://consensys.net/blockchain-use-cases/social-impact/project-unblocked-cash-case-study/. Accessed 08 Aug 2020

51. Bank of Canada, *The Road to Digital Money* (Bank of Canada, Ottawa, 2019). Available at: https://www.bankofcanada.ca/2019/04/the-road-to-digital-money/. Accessed 08 Aug 2020; Reserve Bank of Australia, Submission to the senate select committee on financial technology and regulatory technology (2019). Available at: https://www.rba.gov.au/publications/submissions/payments-system/financial-and-regulatory-technology/index.html. Accessed 14 Aug 2020; CNCEditor, State media sheds light on China's central bank digital currency. China Banking News (2020). Available at: http://www.chinabankingnews.com/2020/04/24/state-media-highlights-regtech-functions-controlled-anonymity-of-chinas-central-bank-digital-currency/. Accessed 14 Aug 2020
52. T. M. Griffoli, M. S. M. Peria, I. Agur, A. Ari, J. Kiff, J. A. Popescu, *Casting Light on Central Bank Digital Currencies*. (International Monetary Fund, Washington DC, 2018). Available at: https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233. Accessed 14 Aug 2020; C. Lagarde, I. M. D. S. F. Festival, Winds of change: the case for new digital currency. IMF . Available at: https://www.imf.org/en/News/Articles/2018/11/13/sp111418-winds-of-change-the-case-for-new-digital-currency. Accessed 14 Aug 2020
53. X. Qiang, President XI's surveillance state. J. Democr. **30**(1), 53–67 (2019). https://doi.org/10.1353/jod.2019.0004
54. L. Schilling, Risks involved with CBDCs: on cash, privacy, and information centralization, in *Conference: Reinventing Bretton Woods: Dialogue of the Continents 2019 Hamburg*, (ResearchGate, 2019). https://doi.org/10.13140/RG.2.2.30645.22248
55. T.J. Gopane, An enquiry into digital inequality implications for central bank digital currency, in *2019 IST-africa Week Conference (IST-Africa)*, (2019), pp. 1–9. https://doi.org/10.23919/ISTAFRICA.2019.8764838
56. M. Killingland, L.B. Dahl, Central bank digital currencies – fad or the future? : A framework for country level assessment of central bank digital currencies (2018). Available at: https://openaccess.nhh.no/nhh-xmlui/handle/11250/2586746. Accessed 14 Aug 2020
57. P. Sandner, P. Schulden, L. Grale, J. Grobe, The digital programmable euro, Libra and CBDC: implications for European banks, in *Conference: EBA Policy Research Workshop: New Technologies in the Banking Sector, Impacts, Risks, and Opportunities*, (2020) Available at: https://www.researchgate.net/publication/343334690_The_Digital_Programmable_Euro_LibrL_and_CBDC_Implications_for_European_Banks. Accessed 16 Aug 2020
58. B. Carson, G. Romanelli, A. Zhumaev, *The Strategic Business Value of the Blockchain Market* (McKinsey, Sydney, 2018) Available at: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value. Accessed 08 Aug 2020
59. Commonwealth Bank, Commonwealth Bank completes new blockchain-enabled global trade experiment (2018). Available at: https://www.commbank.com.au/content/shared/newsroom/2018/07/commonwealth-bank-completes-new-blockchain-enabled-global-trade-. Accessed 16 Aug 2020; J. P. Morgan, J.P. Morgan creates digital Coin for payments (2019). Available at: https://www.jpmorgan.com/global/news/digital-coin-payments. Accessed 16 Aug 2020
60. CGAP, *China: A Digital Payments Revolution* (CGAP (Consultative Group to Assist the Poor), Washington DC, 2019). Available at: https://www.cgap.org/research/publication/china-digital-payments-revolution. Accessed 16 Aug 2020
61. B. Dervishi, A. Falk, D. Therrien, M.O. Bonane, G. Buttarelli, E. Denham, Joint statement on global privacy expectations of the Libra network (2019). Available at: https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf. Accessed 14 Aug 2020

62. D. Marcus, Hearing before the United States senate committee on banking, housing, and urban affairs: testimony of david marcus (2019). Available at: https://www.banking.senate.gov/imo/media/doc/Marcus%20Testimony%207-16-19.pdf. Accessed 14 Aug 2020
63. S. Brown, Brown: Federal reserve must protect economy and consumers from Facebook's monopoly money | U.S. Senator sherrod Brown of Ohio (2019). Available at: https://www.brown.senate.gov/newsroom/press/release/brown-federal-reserve-must-protect-economy-and-consumers-from-facebooks-monopoly-money. Accessed 16 Aug 2020
64. Libra, n. d., Libra | A new global payment system, Libra.org (2020). Available at: https://libra.org/en-US/. Accessed 14 Aug 2020
65. H. Murphy, K. Stacey, M. Kruppa, D. Lee, Facebook Libra: the inside story of how the company's cryptocurrency dream died. *Financial Times*. Available online: https://www.ft.com/content/a88fb591-72d5-4b6b-bb5d-223adfb893f3. Accessed 03 Mar 2022
66. V. Buterin, Trust models. Vitalik.ca (2020). Available at: https://vitalik.ca/general/2020/08/20/trust.html. Accessed 30 Nov 2020
67. R. O'Dwyer, Blockchains and their pitfalls, in *Ours to Hack and to Own*, ed. by T. Scholz, N. Schneider, (OR Books, New York City, 2016), pp. 228–232
68. S.L. Star, The ethnography of infrastructure. Am. Behav. Sci. **43**(3), 377–391 (1999). https://doi.org/10.1177/00027649921955326
69. C. Troncoso, M. Isaakidis, G. Danezis, H. Halpin, Systematizing decentralization and privacy: Lessons from 15 years of research and deployments, in *Proceedings on Privacy Enhancing Technologies*, (2017), pp. 302–329. Available at: https://arxiv.org/abs/1704.08065. Accessed 12 June 2020
70. V. Dhillon, D. Metcalf, M. Hooper, The DAO hacked, in *Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You*, (Apress, Berkeley, 2017). https://doi.org/10.1007/978-1-4842-3081-7_6
71. Least Authority, Ethereum 2.0 specifications security audit report Ethereum foundation (2020). Available at: https://leastauthority.com/static/publications/LeastAuthority-Ethereum-2.0-Specifications-Audit-Report.pdf. Accessed 16 Aug 2020
72. E. Alston, W. Law, I. Murtazashvili, M. B. H. Weiss, Can permissionless blockchains avoid governance and the law? (2020). Available at: https://doi.org/10.2139/ssrn.3676761
73. Library of Congress Law, Regulation of cryptocurrency around the world (2018). Available at: https://www.loc.gov/law/help/cryptocurrency/world-survey.php. Accessed 16 Aug 2020
74. T. Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (Harper Business, New York, 2000)
75. J. L. Marechaux, Towards advanced artificial intelligence using blockchain technologies—IEEE blockchain initiative (2019). Available at: https://blockchain.ieee.org/technicalbriefs/march-2019/towards-advanced-artificial-intelligence-using-blockchain-technologies. Accessed 16 Aug 2020
76. K. Salah, M.H.U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: Review and open research challenges. IEEE Access. **7**, 10127–10149 (2019). https://doi.org/10.1109/ACCESS.2018.2890507
77. T.N. Dinh, M.T. Thai, AI and blockchain: A disruptive integration. Computer **51**(9), 48–53 (2018). https://doi.org/10.1109/MC.2018.3620971
78. N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety* (The MIT Press, Cambridge, MA, 2012)
79. E. Harris-Braun, N. Luck, A. Brock, Holochain scalable agent-centric distributed computing DRAFT (ALPHA 1) – 2/15/2018. [Online] (2018). Available at: https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf. Accessed Jan 2021
80. Dat Protocol, How Dat works (2019). Available at: https://datprotocol.github.io/how-dat-works/. Accessed 16 Aug 2020

Index

K. Daimi et al. (eds.), *Principles and Practice of Blockchains*,
https://doi.org/10.1007/978-3-031-10507-4