EAI/Springer Innovations in Communication and Computing

K.M. Baalamurugan · S. Rakesh Kumar
Abhishek Kumar · Vishal Kumar
Sanjeevikumar Padmanaban *Editors*

Blockchain Security in Cloud Computing

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series Editor

Imrich Chlamtac
European Alliance for Innovation
Ghent, Belgium

Editor's Note

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

K. M. Baalamurugan
S. Rakesh Kumar • Abhishek Kumar
Vishal Kumar • Sanjeevikumar Padmanaban
Editors

Blockchain Security in Cloud Computing

EAI
RESEARCH MEETS INNOVATION

Springer

Editors
K. M. Baalamurugan
Plot No. 2, Yamuna Expy, Opposite
Galgotias University
Greater Noida, Uttar Pradesh, India

S. Rakesh Kumar
Plot No. 2, Yamuna Expy, Opposite
Galgotias University
Greater Noida, Uttar Pradesh, India

Abhishek Kumar
Computer Science & Engineering
Department
Chitkara University
Solan, Himachal Pradesh, India

Vishal Kumar
Bipin Tripathi Kumaon Institute of
Technology
Almora, Uttarakhand, India

Sanjeevikumar Padmanaban
CTiF Global Capsule, Department of
Business Development and Technology
Aarhus University
Herning, Denmark

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-70500-8 ISBN 978-3-030-70501-5 (eBook)
https://doi.org/10.1007/978-3-030-70501-5

Editing a book is harder than I thought and more rewarding than I could have ever imagined. First and foremost, I would like to thank my father Mr. Krishan Dev Pandey and my mother Mrs. Veena Pandey. Also, my gratitude to my elder sister Mrs. Arpna Tripathi, who always stood by me during every struggle and all my successes.

Also, I'm eternally grateful to my wife Mrs. Kajal Pandey for standing beside me throughout my career and the of writing this book. I also thank my wonderful son Aarudra Pandey, for always making me smile.

Last but not least, I would like to thank my grandparents Late Shivshankar Pandey and Late Kunti Devi.

Dr. Abhishek Kumar
Chitkara University,
Himachal Pradesh, India

In Memory of
Late A. Kaliyaperumal

Dedicated To Parents
Dr. K. Manoharan
Mrs. M. Indira

Preface

The purpose of this edited book is to explore the concepts and techniques of cloud security using blockchain. Also, the possibility of applying blockchain to provide security in various domains is also discussed. The specific highlight of this book will be focused on the application of integrated technologies in enhancing cloud security models and its challenges. This book will stimulate the minds of IT professionals, researchers, and academicians towards further revolution in technologies. The wide variety of topics offers readers multiple perspectives on a number of disciplines. The book is organized into 13 chapters, as discussed in the below paragraphs.

Chapter 1 presents a detailed description about blockchain technology followed by privacy and security. Then, network servicing protocols employed are also described. The distributed database and its drawback, like unreliability, and intermittent or non-existent nodes lead to data conflicts. Being able to deal with conflicts is the fundamental difference between standard distributed databases and blockchains. Resolution of conflict, verifying the transaction and transaction auditability, i.e., consensus, is a core function of blockchains.

Chapter 2 provides the aids and effects of blockchain technology in the industry, blockchain technology industry applications, the significance of blockchain technology and decentralization in industry, and a comparative study on different industry applications to expand the usage of blockchain technology.

Chapter 3 explores the key open problems and challenges experienced while conducting digital forensic processes in blockchain technologies. Then, design science research (DSR) to achieve the objectives of this study is described. Furthermore, the high-level solutions to the identified problems and challenges are also described.

Chapter 4 describes distributed computing. Distributed computing in blockchain works under decentralized public ledger; its technology consists two different methodologies – public blockchain and private blockchain. This chapter also explains the importance of distributed computing in blockchain, platforms, and barriers, as well as its privacy challenges.

Chapter 5 proposes the Ethereum blockchain in the first place, and then the types of blockchain and which one to adapt for each case. The third section is about the

integration of cloud and blockchain, where we are going to detail the benefits and vulnerabilities of the integration and present an example of Azur blockchain.

Chapter 6 presents an outline and structure of blockchain and its various applications in IoT. Blockchain technology helps in building trustless and efficient secure environments in IoT. Therefore, it is necessary to target the basic shape of this technology and explain its use and applications in IoT in a concise and comprehensive manner. This chapter begins with an introduction of blockchain and IoT supported by its working in various applications of IoT. This chapter will provide a user with the fundamentals for understanding blockchain technology in IoT applications.

Chapter 7 deals with blockchain advancement that has expanded to a great deal of thought in IoT courses of action. Its fundamental use circumstances are in the budgetary space, where blockchain makes an encouraging request world and can be used to understand security and assurance issues. In any case, this rising development has an unfathomable potential in the most different mechanical domains and would altogether be able to help achieve the Internet of Things see in different points of view, extending the restriction of decentralization, empowering interchanges, enabling new trade models, and allowing self-administering coordination of the devices.

Chapter 8 proposes an encryption system using verifies signature (VS) in health records. Encryption is used in the cloud. To meet the requirement of blockchain in distributed systems, we construct a verifies signature (VS) scheme with multiple authorities. Taking advantage of VS with the blockchain technology, this proposal could preserve the privacy of patients and maintain the immutability of medical records. This project proposed a VS scheme with multiple authorities in a medical records system, and the number of the bilinear pairing involved in signing is linearly increased with the number of authorities. The primary challenge for multiple authorities is collusion attack. To address this risk, a pseudorandom function seed is shared in every two authorities and preserved secretly. Moreover, in KeyGen, the private key of each authority is embedded into the private key of the patient. According to this, the protocol resists N-1 corrupted authority's collusion attacks. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the enforceability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies.

Chapter 9 explores the proposed novel architecture for managing and sharing electronic medical records (EMR) of patients by various medical entities. As large amount of records is to be handled, the healthcare records are stored in the cloud for simplifying access and sharing of information among different stakeholders. Also, there is a provision to enable security and privacy measures in cloud architecture. Suitable public key cryptography and hashing mechanisms are exploited to keep track of the historical transactions corresponding to the distributed patients' records while preserving confidentiality, integrity, and availability. It also prevents the modification or falsification of data by unauthorized users. Using blockchains, patients' records can only be appended to the database, but not removed. New information can be securely linked to the previous record using cryptographic hashing. Special node called data validator is used to check the quality and authenticity of

user-uploaded data, from which the records can be examined and patient health status reports prepared. Again, encryption and digital signing are performed on the data to store it back into blockchain. Hence, this proposed system will ensure that no single party can modify or tamper with the verified stored records. Our proposed novel architecture was tested against MIT-BIH Arrhythmia dataset and the stated functionality requirements were met.

Chapter 10 examines the impact of blockchain technology in agriculture and food supply chains, presents existing ongoing projects and initiatives, and discusses overall implications, challenges, and potential, with a critical view over the maturity of these projects. Our findings indicate that blockchain is a promising technology towards a transparent supply chain of food, with many ongoing initiatives in various food products and food-related issues, but many barriers and challenges still exist, which hinder its wider popularity among farmers and systems. These challenges involve technical aspects, education, policies, and regulatory frameworks.

Chapter 11 provides a systematic survey of blockchain, its workings, its characteristics, its applications, and challenges of the technology. The aim is to investigate how blockchain technology along with artificial intelligence and the Internet of things would be an effective factor to fight the current pandemic scenario. At the end, a brief survey is carried out on how blockchain technology would be fruitful in uplifting the global economy in the post-Covid world with a summary of the blockchain toolkit by the World Economic Forum.

Chapter 12 addresses everything about blockchain technology along with the issues related to information in healthcare as well as comparison of works, providing deep insight into the issues and solutions. The chapter also provides a survey on existing solutions along with good research ideas for upcoming researchers in the field. Finally, advantages along with the disadvantages of the works available so far have been discussed.

Chapter 13 proposes a system to an application using blockchain with stringent authentication. By considering authentication problem, SADS application is proposed. SADS stands for Stringent Authentication and Decentralized Storage using blockchain. Stringent authentication is the process of providing high-security protocols to the network with the help of cryptographic SHA-256 hash algorithm. This application can be implemented using Ethereum blockchain technology. Decentralized storage is utilized for blockchain. Decentralized storage can be defined as process in which breaking up the storage records takes place from one major server to the multiple servers. This allows fast contact to medical information and it also helps to further research.

Greater Noida, Uttar Pradesh, India — K.M. Baalamurugan
S. Rakesh Kumar
Solan, Himachal Pradesh, India — Abhishek Kumar
Almora, Uttarakhand, India — Vishal Kumar
Herning, Denmark — Sanjeevikumar Padmanaban

Contents

Introduction

Cloud computing is an emerging technology in recent decades and has numerous features like high scalability, reliability, flexibility, and dynamic property. Cloud computing is cost effective, and almost all IT sectors are moving to the cloud. The enormous growth as well as demand of cloud computing lead to a major concern regarding its security and privacy, which is determined by the policies, controls, and technologies needed to safeguard information, applications, and also the related infrastructure of cloud computing.

The use of blockchain technology has been increasing recently due to the level of security it provides. As blockchain uses distributed database, tampering of data is much tougher. The data are encrypted according to a rule and operated in computers that run the blockchain software. Bitcoin is an electronic currency using blockchain technology. Blockchain can increase the security in various domains.

This book explores the concepts and techniques of cloud security using blockchain. Also, the possibility of applying blockchain to provide security in various domains is also discussed. The specific highlight of this book will be focused on the application of integrated technologies in enhancing cloud security models, use cases and its challenges. This book will stimulate the minds of IT professionals, researchers, and academicians towards fourth-revolution technologies.

Finally, the rapid growth and stability of blockchain is going to be key a differentiator for the world of security. This book is going to explicitly address the deadly combination in realizing the importance of security features that can be implemented in cloud computing. The main objective of this book is to promote both practitioners and researchers to share their opinions and recent research in the convergence of these technologies among academicians and industry people. The contributors are expected to present their technical evaluation and comparison with existing technologies. The theoretical explanation and experimental case studies related to real-time scenarios are expected.

Blockchain Security

Satya Prakash Yadav

Abstract Blockchain is a technology of Bitcoin which has developed many applications in finance, trade, telecommunication, and manufacturing. This technology was launched in 2008. It was the brainchild of a bunch of people who are popularly known by the pseudonym Satoshi Naskamoto. Bitcoin has developed a popular cryptocurrency and has covered as a virtual money source for market capitalization. Blockchain is a chain of blocks as appears by the name but has a deeper significance. The context of the words "block" and "chain" refers to digital information (the "block") stored in a public database (the "chain"). Taking note of the distributed database and its drawback like unreliability, intermittent or non-existent nodes lead to data conflicts. Being able to deal with conflicts is the fundamental difference between standard distributed databases and blockchains. Resolution of Conflict, verifying the transaction and transaction auditability, i.e., consensus, is a core function of blockchains.

Keywords Blockchain · Security · Trust · Transparency · Distributed · MPT · Merkle tree · Blocks · Permissioned · Distributed consensuses

1 Introduction

A blockchain has three important parts where "blocks" on the blockchain are made up of digital pieces of information: Any transaction relating to data, time, and the value of dollar which can be purchased from Amazon (just for example sake) is stored in a block. Information about the participant of the transactions is stored in the blocks. Any purchase made in large quantity from Amazon will have the name recorded on Amazon.com. The record made is not about your real name; it captures information with a unique "digital signature," which works as a username. A hash

S. P. Yadav (✉)
Department of Information Technology, ABES Institute of Technology (ABESIT), Ghaziabad, India
e-mail: satya.yadav@abesit.in

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_1

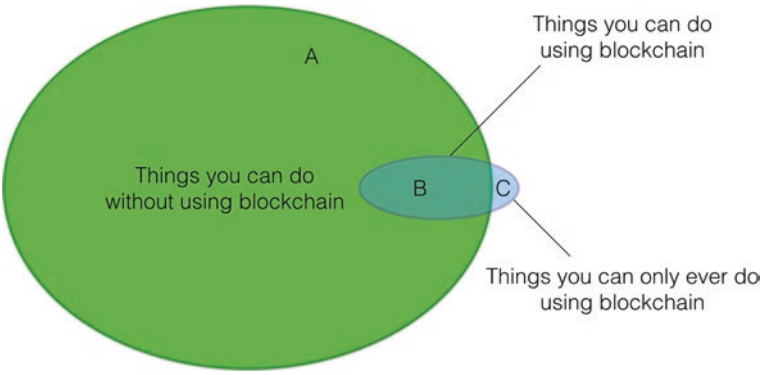


Fig. 1 Venn diagram depicting blockchain utility [2]

code is given to each block. This code is what distinguishes them from other blocks. Just like names that are a person's identifying feature, a hash works in a similar way [1]. For example, you made huge Amazon purchase, but while it's in transit, you decide you just can't resist and need a second one. It might appear that a code will have same information because of the name, but because each block is unique hence each transaction can be stored separately.

The example stated of Amazon might appear that a block is small storage piece, but in reality a single block of blockchain can store 1 MB of data (Fig. 1).

The main property of blockchain is its ability to be shared across boundaries without the need of any central administrator. Proof of validation and authorization proof are the factors that cater to this property. The blockchain transaction carries certain application logic which is centralized and helps the transactions to be processed independently with the help of number of nodes, and this mechanism of consensus helps to keep all nodes in sync.

Blockchains offer the ability to store data with cryptic synchronization. It can be seen that any kind of database is physical entity in the sense that it is able to store large data with know-how of when and where. The storage needs trust which any organization first takes into account [3]. Unlike traditional databases where human dependence plays critical factor, the blockchain provides for security by way of hash codes which once written becomes a lot cheaper than a human resource.

2 Privacy of a Blockchain

Since Bitcoin which resorts to blockchain technology is a virtual money technology, the privacy of the currency is questionable, since anyone can easily view because the users have a choice to connect their blockchain to a computer which is on the network. As a result of automatic iodation, a new bullock is added every time any changes are made, and it is analogous to a newsfeed which appears on social media

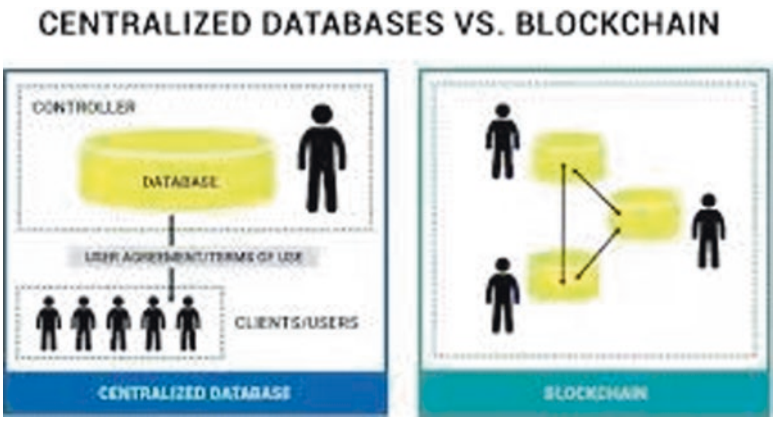


Fig. 2 Centralized databases vs blockchain [4]

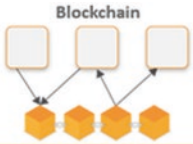
websites. Thus a blockchain has million copies in the network; these copies prevent the manipulation of a Bitcoin difficult. Hence if a hacker tries to change the blockchain, it has to do so on every copy that is available on the network, which is not possible. The anonymity of the Bitcoin blockchain in maintained by the digital signature which makes it even secure.

The anonymity feature gives rise to another crucial question: If you cannot identify who miss adding blocks to blockchain, then how can you trust the technology which is catering to a wide network and to millions of users? (Fig. 2)

The process of adding the records of transactions to the ledger of previous transactions also referred to as the blockchain is called as Bitcoin mining. A ledger appears as a chain with blocks connecting in linked list manner. A chain is thus a track that stores the number of transactions that have taken place till date. In a blockchain, the chains give a fair idea of the transactions that has happened in the past, and any attempt to reuse the coin is easily reported. A traditional database has many advantages [5]. Robustness and persistence: The structuring of nodes makes it possible that the network never falls apart and the data is distributed through the nodes. Resistance to fraud and censorship: The chaining of hashes and the results which are consensus can verify the party that has created any malice or tried to change the data over the security of the network. A common perspective to blockchain technology is attributed to the following assumptions:

- *Blockchains are useless* because decentralization with replication is easier as and you can and sharing in MongoDB clusters or Cetus Data in Postgres.
- *Blockchains are useless* because the differentiating concepts used in blockchain mainly hashes, and proof of work (will be discussed in detail later) are not new. These concepts are applied by Git which is a rate-limiting algorithm and has nothing new to offer (Fig. 3).

Distributed databases are the ones with multiple nodes and on it performing operations. However, in real world the distributed system undergoes many issues



Properties	Blockchain	Traditional Database
Operations	Only Insert Operations	Can perform C.R.U.D. Operations
Replication	Full Replication of block on every peer	• Master-Slave • Multi-master
Consensus	Majority of peers agree on the outcome of transactions	Distributed transactions (2 Phase Commit)
Invariants	Anybody can validate transactions across the network	Integrity Constraints

Fig. 3 Blockchain vs traditional databases [6]

ranging from power failure, partition over long networks, and switch failures. Even though the network on which the message traverses is Ethernet and is strongly connected, it does not guarantee because of the following issues:

- Lost message on the medium
- Excessive wait time in the queue
- Crashing of the remote node
- A temporary pause at a remote node
- Receiving of message at remote node but the response gets lost at the network

3 Security of Blockchain

A new block makes entry in the blockchain in a linear fashion both linearly and chronologically which is toward the end. A typical Bitcoin blockchain will have a position on the chain which is called the "height" [7]. The unacted dated as noted on February 2019 is that the highest height noted was 562,000. To go back and later the contents of the contents of the block in the blockchain is difficult because of a high security hash code which is generated using mathematical function which changes the digital signature into a string of numbers and letters. If the series changes, then the hash code also alters, thereby modifying the entire process and making it invalid. Any change made to the hash will affect the entire blockchain because a block is attached to a previous node which is old. The hacker will have to make changes to the entire height to keep track of uniformity, and as is obvious, this process is not humanly possible. Even if a sincere hacker tries to do so, the process will take huge computing time and power because of the recalculation of the hash codes. Thus altering three information of a block is a difficult task, and therefore a blockchain is secure because of the chain feature. In order to change a single block, a hacker would need to change every single block after it on the blockchain. Recalculating all

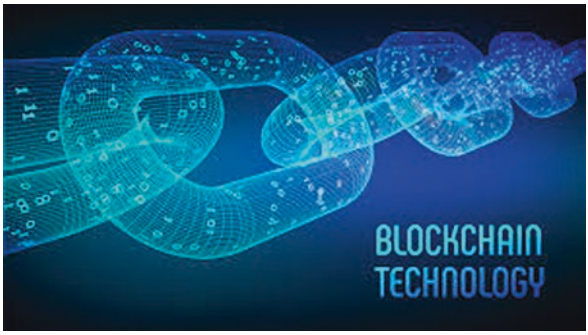


Fig. 4 Chain structuring in blockchain technology [9]

those hashes would take an enormous and improbable amount of computing power. In other words, once a block is added to the blockchain, it becomes very difficult to edit and impossible to delete [8] (Fig. 4).

Blockchains have provided an environment for some of the best features in the technology. However, an important question to consider is the accessibility of the code. Who can read the data? Who can make updates on the data or write? These questions can be answered by considering the public and the private blockchains structure. Let us consider each one of them individually and see what the status of control in a blockchain is.

3.1 Public Blockchain

A public blockchain is a chain without permissions. There is no restriction as to who can or cannot join the network of a blockchain. Anyone can read, write, or participate in the transactional processing of the blockchain [10–12]. The advantage of decentralization comes handy here; it makes sure that once the data has been validated, then no more changes can be made to the blockchain. Examples of public blockchain include Bitcoin, Ethereum, and Litecoin. They are surviving the structure of the technology and easily protect the anonymity of the user. A person owning Bitcoin should have the power to spend it as and when he or she desired. This gives freedom of movement to the cryptocurrency. The following are the advantages of public blockchain.

Open Read and Write
Anyone can make, read, and write transactions on Ethereum or Bitcoin which are the blockchain technologies. These transactions can be easily seen on an explorer of the blockchain.

Ledger Is Distributed
The validation of any transaction can be done by all the nodes of the blockchain; this feature is guaranteed by no centralization which is followed in client-server architecture.

Immutable
Any changes or modification done on the block in a blockchain cannot be altered after validation.

Mining Provides Security
The Bitcoin has the power of the network; it is mining which helps to reduce double spending of the money and prevents any more acts of transaction and its confirmation which can be bogus.

3.2 Private Blockchain

A private blockchain is a blockchain with permissions. These permissions are specifically designed to meet who can or cannot join the network. The transactions they want to become a part of are also in the radar. The aim of a private blockchain is to control the accessibility of the read and write on the data of the transactions [13, 14]. This can only happen once the identity of the person on the network is known. Without an identity, it is not possible to know who made changes that ultimately validated and reflected in the ledger. Platforms that use private blockchain concept include Hyperledger, Hashgraph, and Corda. Advantages of a private blockchain are as follows:

*Permission by Enterprise***:** An enterprise is the one which controls the permissions given to private blockchain.
*Translation Speed is Fast***:** Since now the number of nodes participating is limited, the speed of read or write on the data automatically increases.
*Improved Scalability***:** An enterprise is at the advantageous end because they can add or delete nodes as per the demand; hence, scalability improves.
*Compliance Support***:** An enterprise follows certain rules that are supposed to be adhered to; a compliance support helps to achieve it in this network**.**
*Efficient Consensus***:** The private blockchains follow different census algorithms like BFT POW. Because they have less number of nodes hence consensus is easier (Fig. 5).

One of the major requirements for a good database is its ability to be transparent without giving out crucial information. Blockchains does this by giving full visibility into the following:

- The current state of the database
- The transactions and the modifications made on it
- The origin of a transaction available through digital signature

Traditional databases help to achieve this by making changes on one central location, and request to modify that part of the database which is made on that central location ethic can be either accepted or rejected. These features are called read control or write control. On the other hand, blockchain is write controlled only; to

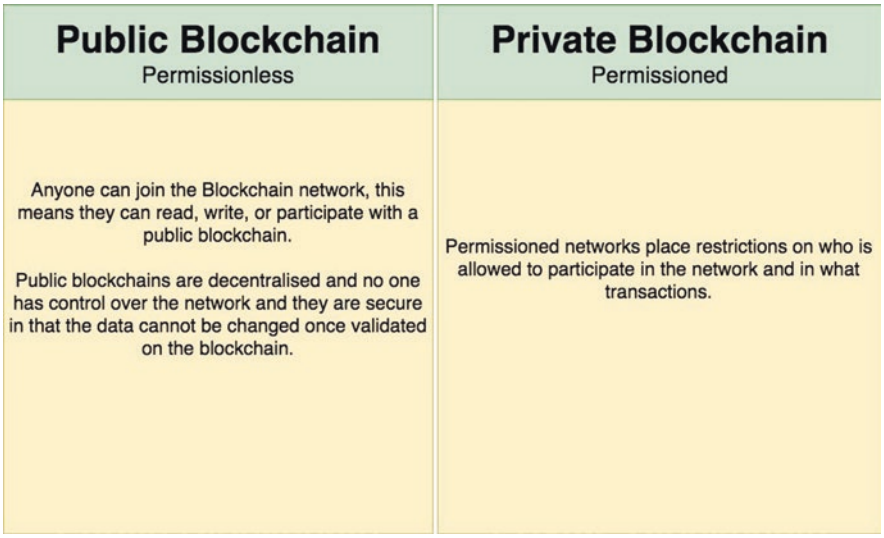


Fig. 5 Private vs public blockchain [15]

mitigate these issues, cryptographic techniques like confidential transactions and zero knowledge proofs can be developed, but the more the hiding, the more will be the computational burden.

3.3 Robustness

The blockchain-based databases are completely fault tolerant, because each node has every transaction and is not limited to just one. The nodes are connected in a peer-to-peer fashion avoiding sudden halts. The blockchain has the ability to make those nodes alive and be updated with the data which were missed.

Blockchains have their own way of dealing with replication which occurs in regular databases. There is no need for configuration; one just needs to connect blockchains with its nodes together which further align to be in sync. Nodes can be easily added or deleted, and the new information flows automatically to other nodes [16].

In a regular database, robustness is maintained by making backup of the data, in case of failure of the architectural structuring, such that the replicated database becomes the new database until the primary one restores. This is an expensive procedure of recovering from the disaster. Blockchains however are connected peer to peer densely and ensure consensus. Since the blockchains have copies across each node on the network, the failure of intermediate nodes goes unnoticed. This method is low cost and maintains redundancy and is followed by Google.

Performance: even though the blockchain technology has many benefits, it still has slower processing power than regular databases because it is optimized. It does the same work as regular database but along with additional burdens [17]:

1. *Verification of signature*: ECDSA technique is used for signing a blockchain transaction digitally. This is just because the nodes are being shared in a peer-to-peer manner. Its verification is a complex process which in irregular database is easier because verification happens only once.
2. *Consensus mechanism*: It is not necessary that all transaction will be processed back and forth at one location. The consensus mechanism deals with forks and how they rollback. In regular databases, there is more worry about conflicted and aborted transactions.
3. *Redundancy*: In a regular database, the performance is solely dependent on each node, but in the case of blockchains, the transactions are distributed equally across the entire chain of blocks; this requires more synchronization.

An important consensus mechanism is proof of work (POW). It was firstly used by Bitcoin which made it popular enough to be adopted by other cryptocurrencies as a consensus mechanism. The process in the proof of mining is referred to as mining, and the nodes which form the chain are called the miners. A complex mathematical problem in the form of puzzle is presented to the miner. As soon as the miner solves that puzzle, it has the power to add a block to the chain as a reward.

4 Network Servicing Protocol

The main aim of the protocol in Bitcoin production is to make sure that the same Bitcoin is not used in the same transaction at the same time; otherwise, it leads to confusion, and the detection becomes difficult. Each Bitcoin can act as gold, their base unit is Satoshi which is supposed to be unique and has a value attached to it. Each Bitcoin has a history associated with it which stores all the transactions that have taken place on it by making use of the proof of work mechanism [18]. The CPU power has a lot to say in this; it decides to accept or reject a new block in the chain. As soon as all the nodes which are acting as miners come at a common solution, a new block is added to the chain. This block has a timestamp which can also include messages or some form of data (Fig. 6).

Blockchain is used to create a digital ID for each property, allowing it to be traced across the network. Except creating the $64,000 estate market a lot of liquid, strictly from a loan application perspective, this digital ID would come with a sequence of possession and current market valuation which will permit banks to quickly verify this ownership standing or make sure of the value, mitigating the necessity of browsing title deeds and interacting with surveyors. Different hardware used by the miners for mining is as follows:

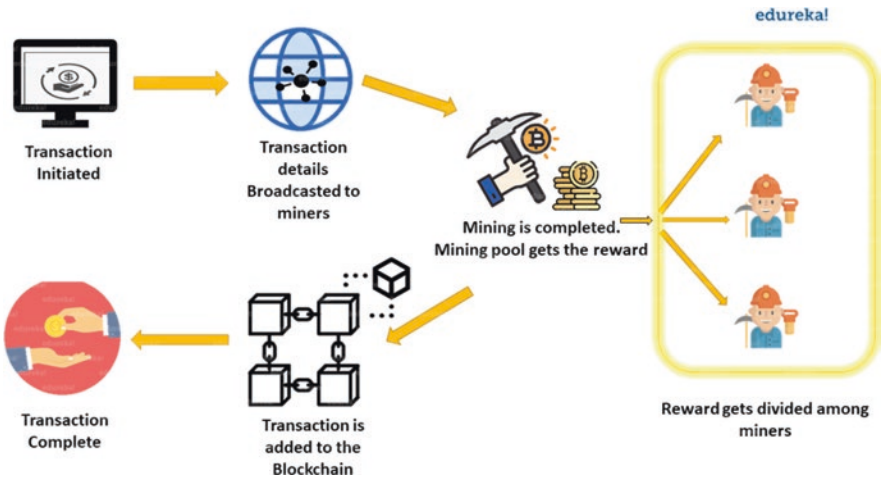


Fig. 6 Blockchain mining hardware [19]

CPU Mining: The proof of work consensus protocols used to validate a transaction using a normal computer.

GPU Mining: This is almost similar to CPU mining, with an addition. It uses graphic cards; these cards provide more functionality and less electricity usage.

FPGA Mining: Also known as "field-programmable gate array mining." It is a circuit-based task making the process of inning faster than processes operating normally.

ASIC Mining: Is an "application-specific integrated circuit," which modifies a circuit as per the requirements. Asics performs better than CPUs, GPUs, and FPGAs in both speed and efficiency; hence, their usage is limited to Bitcoin mining.

Mining Pools: The successful mining of a block is increased by many folds by pooling together resources. The miners list how much each has contributed and also the rewards that can be further gained.

Cloud Mining: Another approach is where miners rent their work to other miners, and they are supposed to process the task in a given time frame.

As discussed in our previous topics, it is obvious that the identity of the sender is not visible, thereby making transaction on Bitcoin anonymous. The sending of Bitcoins and then receiving the value are often done under pseudonym. This pseudonym stays in the data file, and any updating made on the block is sent on this address. This address is linked to the sender for further updates. The idea to create a new pseudonym for every new transaction would be cumbersome; hence, it was not applied. There are many reasons which make Bitcoin anonymous, the first one being that just as our banks hold one unique identity for our accounts, a Bitcoin does not follow the same approach. For transaction to take place, the Bitcoin addresses with an associated private key can be generated without any personal information about the sender attached to it. The second interesting point is the sender and

receiver are unaware about the personal information of each other. The Bitcoin transaction works on the address and private key only. The third point is since the Bitcoin follows blockchain technology, a single block receives information which is easily forwarded to the next block, and there is no knowledge about the initial identity needed. However, it is not a difficult task to check the anonymity in case of undue circumstances, since we are dealing with money. We can look into two major points: the first is because the value in one block has traversed across a network, so by tracing the multiple nodes or blocks we can check. The data collected from multiple sources can be used to trace the origin. The second method is that it is often seen that the address generated for a transaction includes a combination of real identities. The address which is used to deposit and receive money is included through a regulated exchange like a wallet or a donation that was made publicly, for example, payment made to online store [20, 21]. The transparency of transaction is an advantage offered by Bitcoin technology has the benefit of transaction transparency, and the various number of addresses used can be clustered and connected to a single user, making deanonymizing the user simple.

5 Distributed Consensuses

A distributed system includes different set of processes mainly computers which pass, messages to each other, and have a mechanism to coordinate a common objective; in this case, it could be a mathematical problem. The group of computers that are connected together work for a common goal. A distributed system is a group of computers working together to achieve a common goal. Even though the systems are separate, they appear to show one unified goal (Fig. 7).

Distributed computing technology has contributed immensely to the development of the blockchain technology. Essentially, a blockchain is a new type of distributed system. It came into light with the inset of Bitcoin and ever since has used the technology to further strengthen the effect in a distributed environment [23]. Hence to know how blockchains work, an understanding of the principles of distributed systems is required. The filed is vast and a lot of research in this area of distributed computing has already taken place and continues to do. The umpteen numbers of architectures in the computer make it even difficult to understand how the environment in a blockchain actually responds. Features of a distributed system are as follows:

- Components of the distributed system are concurrent. It gives way to resource sharing which includes systems that are on the network at the same time.
- The different components will be autonomous.
- A distributed system works without a global clock and is spread across vast geographies.
- Fault tolerance is comparatively more in a distributed system, thus more robust.
- The ratio of price/performance is considerably improved.

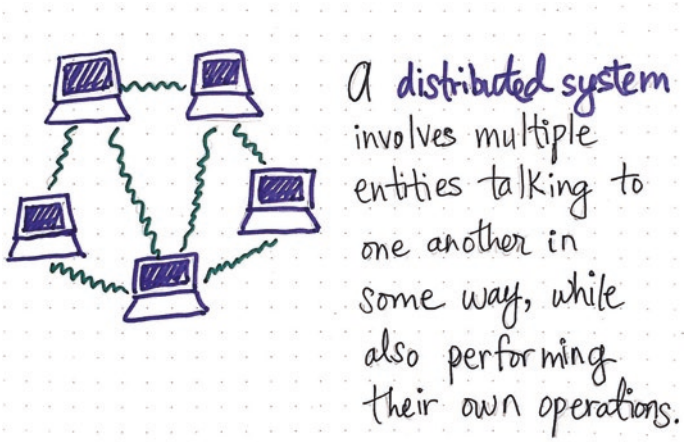


Fig. 7 A distributed system [22]

A distributed system achieves the following goals:

- *Transparency*: Ability to know about different systems, their location migration, concurrency, failure, and relocation.
- *Openness*: Ability to make changes to the system easily.
- *Reliability*: Capability to mask errors and be able to withstand failure without affecting the overall network.
- *Performance*: Since dependence is not a single computer, the performance of a distributed system is better.
- *Scalability*: Distributed systems should be able to expand across different regions with respect to the administration and the size.

5.1 Effect of Consensus on Distributed Computing

Transaction validation sets up at the beginning of any transaction which is published on the network. It makes sure that all the rules that verify the mathematical relations are conformed or not. *Transaction confirmation* process takes place as soon as the transactions published are created in a block which then becomes a part of the larger blockchain. *Block validation* is for a node to be added to a block; it is made sure that it is validated by all the members of the Bitcoin network. It is checked for the right protocol and then only added else rejected.

Vitalik Buterin is the one who launched the platform for the world's largest cryptocurrency called as Ethereum in July 2015. The platform aims to enable an open distributed network for introducing their own decentralized applications (DApps). The peer-to-peer payment system of Bitcoin technology if applied can be used for making use of Ethereum for its program code execution over a decentralized virtual

machine (EVM). Every time a miner makes some changes on a block, a fee is charged for it. The network miners decide as to which block will make its entry in the ethereal blockchain over the network. The transaction fee that is calculated for the action performed is called as gas and paid for in Ether. Thus for a given Ethereum network, the gas works as a fuel which functions to make transactions, for data storage for executing smart contacts, and for launching DApps. The gas limit is the total amount that the person is willing to put for the transaction taking place for Ether, thereby confirming the value of the transaction. The range of values for gas limit holds a certain meaning. The higher a value of gas limit is, the more computational cost needs to be applied for executing the smart contract. The minimum limit for this is 21,000 units of gas, which is the standard for Ether-based transfer. The sender has the power to limit the price for each transaction that takes place. The gas price is the amount the user has decided to spend on each unit of gas. The multiplication of the gas limit with the gas price generates a value that is the commission for any Ether-based transaction. For instance, if the gas limit is 20,000 units and the gas price is 10 Gwen, then it means that the sender is ready to spend 0.021 Ether after transaction is executed. If the value of the gas price keeps increasing, then it is an important transaction in the Ethereum network; the unused gas once the transaction is complete is returned to the account of the sender. A low value of gas limit set by the user is rejected as "out of gas" error [21]. The miner however is entitled to receive the payment even though the amount sent by the user may be rejected or not.

6 Merkle Patricia Tree

An MPT is a combination of Patricia tree and Merkle tree, with some additions that improve the overall structuring. To better understand the tree, it is important to consider the two separately.

6.1 Patricia Tree

Patricia tree is a data structure which works as prefix tree or a radix tree. The tree has a key which follows a common path, and it can be used to trace the nodes on the network. It is a simplified approach and hence is easier to calculate and implement. It makes use of routing tables and low specifications of the system (Fig. 8).

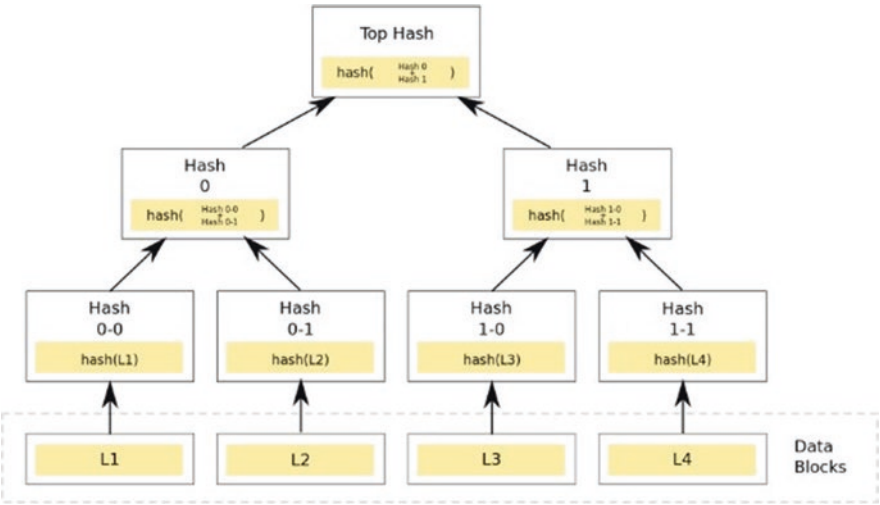


Fig. 8 MPT example [24]

6.2 Merkle Tree

Merkle tree is also referred to as hash tree; it contains hashes. The data is stored at the last nodes also called as the leaf nodes which have no further children. The remaining nodes which are parent nodes contain hash values of their child nodes plus the total sum of the children nodes and their hashed values.

Example of Merkle Tree
Few can check that two different nodes do not carry the same values of hash by the example given below using Merkle tree. First step is to compare the hash values associated with the top nodes; in case they are similar, it means the data is same. In the figure, have a look at the four nodes (L1, L2, L3, L4), look for the top hash values .mow, check Hash 0 and Hash 1, and look for the branch whose data is not the same [25]. Continuing in this manner, it will be easier to find out the node which has similar data (Fig. 9).

Thus, using Merkle tree, we can evaluate the difference in hash values. This feature provides security in the network of blockchains. If any value changes at any given level, then the value at the root level or the top level also changes, thereby depicting the tempering done. The parties can be easily updated about any illegal modification that if at all is made. Thus this feature of blockchain strengthens the system and makes it secure for any industry or organization.

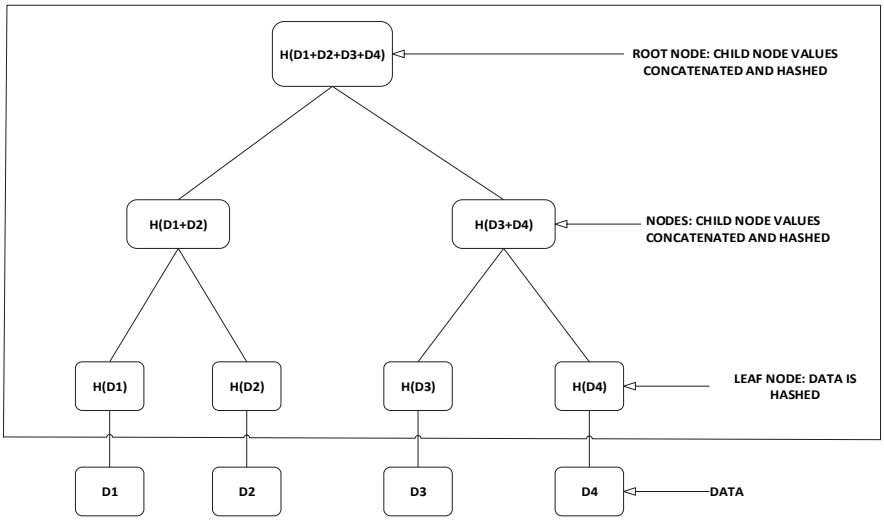


Fig. 9 Merkle tree example [26]

7 Rewards

The term reward in Bitcoin block is the Bitcoin or Bitcoins that are added to a miner in the cryptocurrency network that mine a block of the chain successfully. The miners that create the blocks are given the reward. The value of the reward is the total of block subsidy also referred to as stashes added to the fees of the transaction that was along the block. The size of a block in Bitcoin is 1 MB; it stores information about the transactions. The information, for instance, could be Alice sends money to Baker, and this is stored on the block. Other cryptocurrencies also use the rewarding mechanism where miners are awarded on addition of blocks. In the beginning, each Bitcoin reward had an estimated value of 50 BTC. This value is divvied into half after discovering 210,000 blocks, and this usually happens in 4 years. The current reward value is 12.5 BTC as of February. The reward process follows the cryptocurrency methods where after total 64 iterations and halving the value, the value of the reward comes down to 0.

8 Analysis and Discussions

The blockchain eases this process by improving the overall structure of money transfer. The transaction is stored in a secure distributed ledger. Once the transaction occurs, the receiving party can easily access the payment without the involvement of any third party. A distributed ledger eliminates the unnecessary charges which were made in the traditional method [27]. The security of the process is maintained

by making this whole process irreversible such that no change can be further made in the ledger once a transaction completes. Following major outcomes and scopes can be stated from the current review paper:

1. *Voting*: The traditional method of ballet paper voting has been extensively adopted across the globe. This method presented many disadvantages. Some of them are listed below: long waiting queues at the voting center, the paper method of voting causes delay in result declaration, manhandling of electronic voting machines is possible, and any antisocial elements can rig the booths during the voting process.
2. *Supply Chain*: The ability of blockchain technology to provide tracing feature makes it a good choice for food sector. The industry can know what material to ship and where. The contamination of food at any level can be easily traced. The supply chain can be managed more effectively.
3. *Energy Sector*: The blockchain technology gives way to better energy restoration techniques. It includes sharing energy and its sources with neighbors, making more avenues for business deal possible.
4. *Government*: The UK Government believes that blockchain technology can mitigate corruption by its ability to track unwanted usage of funds. For instance, the student loans can be kept a keen eye on, and then they can also be used to benefit underprivileged students.
5. *Healthcare*: Less use of paper definitely increases the durability of records. It is believed that the confidential documents of health and diagnosis can be stored securely without the fear of hacking or manhandling [28].
6. *Music Industry*: It is hoped that if blockchain is used in the industry, then the earrings generated can be kept track of. The privacy problem can be handled. The cryptocurrency can be used for payment, making the process smooth. The distributors can be a disadvantaged group in this scenario, but the whole divide between payment and issue of rights can be legalized.
7. *Computer Security*: The security breach across a network is common news. Hackers access the network and steal data and often go without being traced. The blockchain technology provides cyber security by providing data that cannot be manipulated, decentralization, and the security at the cryptographic level. Guard time is one such example.
8. *Tax Collection*: The transparency feature of blockchain technology is a two-way road. If it provides a user with the security that they can trace the money they pay in the form of taxes, then even the government can collect taxes by generating invoices based on blockchain. This approach was started in February 2018.
9. *Fine Art Forgery*: The artists across the globe often gave the issue of their work being copied or stolen. To prevent this menace, a US company by the name Versant has decided to apply blockchain technology. The owner of the museum and the artist can make the verification based online following the blockchain technology.

10. *Protection of Endangered Species*: A Uganda-based company has decided to keep track of the geography, the location, and the migration pattern of some species that are endangered. The approach aims to track the above properties through blockchain technology.

The new models that need identity to grow their business rely heavily on the blockchain. The Blockchain when used in decentralized application can be an effective tool. The current scenarios where identities are stored digitally are obviously a good way of data storage, but they are most vulnerable also. The use of digital information can be for functioning of decentralized applications. With a new technology being studied every now and then, the blockchain and how it stores data and how it prevents data theft is also in nascent stage. The focus will be on how viable the blockchain will be.

9 Conclusions

The growing business needs have led to the use of personal information. Some business motives state the need to lure more customers into their business models. Companies often ask for details to sell their products more. This flow of personal data can lead to data theft. Blockchain is the underlying technology paving the path to self-sovereign identity through decentralized networks. It ensures privacy and trust, where transactions are secure, authenticated, verifiable, and endorsed by relevant, permission participants. The problem of consensus in blockchain is of immense importance. It is through the consensus the leader is elected and the network is built. However, the problem of consensus is equally seen in synchronous and asynchronous systems. Most of the real-world problems are asynchronous. The designing of a synchronous model is therefore easier. The synchronous system assumes that communication across the nodes goes round and round. The assumption is that in one round the information flows and the reply is received, without bothering the other processes. Blockchain happens to provide a solution to this age-old practice.

10 Future Scopes

Blockchain makes use of smart contracts which use a single window nationally where only one point of entry is required for trade stakeholders for them to submit documentation for custom procedure. The future of blockchain is bright if the projects that are under research are successfully complete. The blockchain can greatly influence the shipping industry and in international trade, and it can take over. The projects need integration of work and an environment that is regulated enough. Need is also of interoperability and standardization.

References

1. N.T. Courtois, R. Mercer, Stealth address and key management techniques in Blockchain systems. *Proc. ICIS- SP*, 2017, pp. 559–66
2. https://breakermag.com/reddit-ponders-the-venn-diagram-of-blockchain/
3. J. Bonneau et al., Mixcoin, Anonymity for Bitcoin with Accountable Mixes. *Proc. Int'l. Conf. Financial Cryptography and Data SecUrity*, Springer, Berlin, Heidelberg, 2014, pp. 486–504
4. https://intellipaat.com/tutorial/blockchain-tutorial/blockchain-vs-database/
5. L. Valenta, B. Rowan, Blindcoin: Blinded, accountable mixes for bitcoin. *Proc. Int'l. Conf. Financial Cryptography and Data SecUrity*, Springer, Berlin, Heidelberg, 2015, pp. 112–126
6. https://www.quora.com/Whats-the-difference-between-blockchain-and-a-database
7. T. Ruffing, M-S. Pedro, ValueShuffle: mixing confidential transactions for comprehensive transaction privacy in bitcoin, *Proc. Int'l. Conf. Financial Cryptography and Data SECURITY*, Springer, Cham, 2017, pp. 133–154
8. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195
9. https://www.entrepreneur.com/article/306420
10. S.F. Sun et al., RingCT 2.0: A compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency Monero. *Proc. EUROPEAN SYMPOSIUM on Research in COMPUTER SECURITY*, Springer, Cham, 2017, pp. 456–74
11. S.R. Kumar, N. Gayathri, Trust based data transmission mechanism in manet using solsr. In *Annual Convention of the Computer Society of India* (pp. 169–180). Springer, Singapore., S. R., & Gayathri, N. (2016, December). Trust based data transmission mechanism in MANET using sOLSR. In *Annual Convention of the Computer Society of India* (pp. 169–180). Springer, Singapore (2016, December)
12. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
13. K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology. In *Proc. IEEE 18th Int. Conf. High Perform. Comput. Commun, IEEE 14th Int. Conf. Smart City, IEEE 2nd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2016, pp. 1392–1393
14. R.K. Sakthivel, G. Nagasubramanian, F. Al-Turjman, M. Sankayya, Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. Trans. Emerg. Telecommun. Technol., e3947 (2020)
15. https://medium.com/@zhangsanbtc/ending-the-soft-hard-fork-debate-a-safe-hard-fork-is-the-same-as-a-soft-fork-c0e96eeb62d0
16. H. Ethan, F. Baldimtsi, L. Alshenibr, A. Scafuro, S. Goldberg, TumbleBit: An untrusted tumbler for bitcoin-compatible anonymous payments. In *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2017, pp. 1–15
17. H.R. Hasan, K. Salah, Blockchain-based solution for proof of delivery of physical assets, in *Blockchain (Lecture Notes in Computer Science)*, vol. 10974, (Springer, Seattle, Jun. 2018), pp. 139–152
18. H. Hasan, K. Salah, Proof of delivery of digital assets using blockchain and smart contracts. IEEE Access **6**, 65439–65448 (2018)
19. https://www.edureka.co/blog/blockchain-mining/
20. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. Blockchain, Big Data and Machine Learning: Trends and Applications, 97 (2020)
21. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan Future blockchain technology for autonomous applications/autonomous vehicle. In *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles* (pp. 165–177). IGI Global
22. https://medium.com/baseds/many-nodes-one-distributed-system-9921f85205c4

23. E. Heilman, F. Baldimtsi, S. Goldberg, Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions, in *Financial Cryptography and Data Security*, (Springer, Berlin, 2016), pp. 43–60
24. https://en.wikipedia.org/wiki/Merkle_tree
25. J. Liu, W. Li, G. Karame, N. Asokan, Toward fairness of cryptocurrency payments. IEEE Secur. Priv. **16**(3), 81–89 (Jun. 2018)
26. https://www.researchgate.net/figure/An-example-of-Merkle-tree-Each-leaf-is-a-hash-of-one-packet-Each-internal-node-is-the_fig2_220465950
27. M. Mut-Puigserver, M. Payeras-Capellà, M. Cabot-Nadal, Blockchain-based fair certified notifications, in *Data Privacy Management, Cryptocurrencies and Blockchain Technology (Lecture Notes in Computer Science)*, vol. 11025, (Springer, Barcelona, 2018), pp. 20–37
28. R. Chandran, S.R. Kumar, N. Gayathri, Genetic algorithm-based tabu search for optimal energy-aware allocation of data center resources. Soft. Comput. **24**(21), 16705–16718 (2020)

Satya Prakash Yadav is currently on the faculty of the Information Technology Department, ABES Institute of Technology (ABESIT), Ghaziabad (India). He has awarded his Ph.D. thesis entitled "Fusion of Medical Images in Wavelet Domain" to Dr. A.P.J. Abdul Kalam Technical University (AKTU) (formerly UPTU). A seasoned academician having more than 12 years of experience, he has published three books (*Programming in C*, Programming *in C++, and Blockchain and Cryptocurrency*) under I.K. International Publishing House Pvt. Ltd. He has undergone industrial training programs during which he was involved in live projects with companies in the areas of SAP, Railway Traffic Management Systems, and Visual Vehicles Counter and Classification (used in the metro rail network design). He is an alumnus of Netaji Subhas Institute of Technology (NSIT), Delhi University. A prolific writer, Mr. Satya Prakash Yadav has published two patents and authored many research papers in Web of Science indexed journals. Additionally, he has presented research papers at many conferences in the areas of image processing Feature Extraction, Information Retrieval and programming, such as C, Data Structure, C++, C#, and Java. Additionally, he is also the lead editor in CRC Press, Taylor and Francis Group Publisher (USA), Science Publishing Group (USA), and Eureka Journals, Pune (India).

Significance of Blockchain Technologies in Industry

R. S. M. Lakshmi Patibandla and Lakshman Narayana Vejendla

Abstract Blockchain technology is set to extremely affect a wide assortment of enterprises, extending from capital markets to the music business. While some utilization cases may appear glaringly evident, the innovation is as yet encircled by a lot of promotion and vulnerability. As a chief, in what manner would it be a good idea for you to move toward the subject, and when would it be a good idea for you to get the ball rolling and effectively expect to execute blockchain innovation?

As indicated by Juniper Research, six of ten enormous enterprises are either effectively considering or during the time spent sending the blockchain revolution. Among organizations that have arrived at the proof of concept stage, 66% (66 percent) expected blockchain to be incorporated into their frameworks before the finish of 2018. The examination guaranteed that those organizations that would profit most from blockchain incorporate those with the requirement for (1) straightforwardness in exchanges, (2) current reliance inheritance stockpiling frameworks, and (3) a high volume of transmitted data. Taking a gander at the explanations behind actualizing blockchain, there is a characteristic hazard that supervisors anxious to investigate new advancements from a hasty opinion without investigating elective alternatives. As per the exploration, foundational change, as opposed to innovation, may give both better and less expensive answers for the current issue. For some organizations, the go-to way to deal with examining potential use cases for blockchain is to search for wasteful aspects in ebb and flow processes. This approach is ensured to give a few outcomes; however, frequently the arrangement is to genuinely restructure inheritance procedures to fit an advanced world as opposed to investigating new and obscure advances. One motivation behind why blockchain frequently develops as a response to numerous issues is that it is anything but difficult to envision significant level use instances of blockchain innovation. Be that as it may, as we adventure under the outside of such use cases, applying blockchain

R. S. M. Lakshmi Patibandla (✉)
Department of IT, Vignan's Foundation for Science, Technology, and Research, Guntur, AP, India

L. N. Vejendla
Department of IT, Vignan's Nirula Institute of Technology & Science for Women, Guntur, AP, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_2

innovation to a realized issue is very frequently a hypothetical arrangement. On the off chance that we take a gander at it, blockchain in its most straightforward structure is an option in contrast to the customary database. Blockchain varies from a database from multiple points of view, yet the most noteworthy special case is the decentralized idea of blockchain. While a database requires a focal position to keep up and oversee information, blockchain offers a decentralized way to deal with the capacity and check of information. Be that as it may, this element includes some significant pitfalls. Blockchains in their present state make them scale issues, making them slower than customary databases. Likewise, clients must compensation a charge for every "exchange" on the database, which is mutable and inconsistent. This research work provides the aids and effects of blockchain technology in the industry, blockchain technology industry applications, the significance of blockchain technology and decentralization in industry, and a comparative study on different industry applications to expand the usage of blockchain technology.

Keywords Blockchain · Industry · Database · Technology

1 Introduction

A blockchain is, in the most extreme direct of terms, an age submitted plan of steady records of information that is estimated by a social occasion of PCs not constrained by any single segment. These blocks of information (e.g., block) are guaranteed about and bound to one another utilizing cryptographic standards (e.g., chain). For inspectors new to the cryptographic money world, one of the most overpowering and astounding perspectives can be blockchain. Blockchain advancement is the thing that forces and supports the impelled cash space, and different experts recognize that it contains various potential applications and utilizations past cryptographic kinds of money as well. You may have found a few solutions concerning money-related foundations and even standard relationship around the globe investigating ways that they can encourage blockchain improvement into their standard practices [1]. Past that, regardless, it will when all is said and done be somewhat a puzzle concerning what blockchain is truly and concerning how it limits [2]. Underneath, we'll analyze the multifaceted nuances of blockchain, giving a framework of this headway, how it fills in with respect to automated kinds of money and other possible applications, and why it might be one of the most unique signs since the web. Blockchain progression underlies mechanized money structures, and it might in like way be utilized in a wide gathering of different applications also. Blockchain systems private key turn of events and spread sorts out and shared records [3]. Attesting and embracing exchanges is a colossal restriction of the blockchain for modernized money.

Blockchain can be thought of as the mix of a few assorted existing degrees of progress. While these advances themselves aren't new, it is the means by which they

are joined and applied which accomplished blockchain. As demonstrated by CoinDesk, these three-piece developments are the following:

Addressing the movement of private cryptographic keys helps with envisioning two individuals who wish to organize a trade on the web. These individuals hold two keys: one of these is private and one is open. By joining everybody and private keys, this bit of cryptography licenses individuals to pass on a safe pushed character reference point. This ensured about character is an essential piece of blockchain improvement [5]. Together, an open and a private key make a moved engraving, which is an immense gadget for demanding and controlling belonging.

The pushed property of the cryptography piece is then coexisted with the gushed sort out movement part. Blockchain progression goes about as a titanic game plan of individuals who can go about as validators to show up at a perception about various things, including trades [6]. This method is ensured by numerical statement and is used to ensure the framework. By combining the utilization of cryptographic keys with a scattered structure, blockchain considers new sorts of cutting-edge affiliations [7].

One of the most fundamental bits of blockchain improvement is the way that it certifies and supports trades. In the model above, in which two individuals wish to lead a trade on the web, each with a private and an open key, blockchain grants the head (individual A) to use their private key to join information concerning the trade to the open key of the resulting (specific B). This information together structures some bit of a block, which contains a moving imprint likewise as a timestamp and other significant information about the trade, at any rate not the characters of the individuals pulled in with that trade [8]. That block is then transmitted over the blockchain framework to the whole of the center centers, or other part segments of the structure [9], which will by then go about as validators for the trade.

The aggregate of this sending of information and inclining toward blocks requires titanic degrees of figuring power. In sensible terms, it may emanate an impression of being dazzling to envision that unlimited PCs around the world should all be tense to submit managing power and various resources for this endeavor [10]. One response for this issue for the blockchain sort out is mining. Mining is related to a standard cash-related issue called the "extreme aversion of the hotel." This thought summarizes a condition wherein individuals who each show freely in their unique issues will everything considered carry on in inclinations in spite of the upside of the entire of all customers because of debilitating a preferred position through their movement at a full scale level [11]. During the time spent blockchain guaranteeing, an individual who gives up a little piece of their computational power to offer help to the framework along these lines secures a prize. Through carrying on of good duty (expecting to get the prize: for this circumstance, an unassuming proportion of cryptographic cash), that individual has been reinforced to help serve the necessities of the wider framework [12].

For blockchain structures, this is a fundamental improvement toward ensuring that uncommon money-related structures can't be spent in various trades simultaneously, a thought known as twofold spending. To guarantee against twofold spending, blockchain frameworks need to ensure that motorized cash-related structures

are both strikingly guaranteed and penetrated with deference. One strategy for offering this help is to have the concentrations inside the blockchain structure go about like bits of the record structure itself, keeping up a past piled up with trades for each coin in that engineer by endeavoring to manage bewildering numerical issues [13]. This center centers serve to certify or exonerate blocks tending to bits of information about trades. In case a more prominent piece of center point overseers appears at a relative response for an issue, the block is confirmed, and it is added to the chain of stops that exist before it. This new block is time meandered and is likely going to contain information about various bits of past trades. This is the spot where there is space for blend depending upon the particular structure: some blockchain frameworks audit express kinds of information for their blocks, while others consolidate different methodologies of information [14].

It is this last piece of the blockchain that a few people perceive gives the most potential to future applications later on. The data making up upsets in a blockchain, for instance, the one identifying with the Bitcoin sort out, for example, is identified with the past trades that have happened between different individuals, going about as an open record of each and every previous trade. In any case, the data identified with blocks could be anything. For governments, for example, portions of blockchain movement may show solid concerning grasping trades, which is routinely done through reliable structures. Blockchain headway could be significant for giving outline trails or to grow another association between different cash-related foundations and likely decoration [15]. For various bits of the cash-related world, blockchain may have the decision to streamline the path toward clearing and reimbursement, which has commonly taken days. This improvement could in like manner help with robotizing authoritative consistency by making understanding of the genuine piece into code, for example, or by permitting unequivocal sorts of trades and blocking others. There are wide-going open doors for blockchain progress both inside and outside of the budgetary world.

Similarly, as with any innovation, be that as it may, it's not so much clear how to best utilize the groundbreaking abilities of blockchain. Over the long haul, all things considered, proceeded with experimentation, will uncover better approaches for using blockchain for a wide range of purposes, just as new strategies for using blockchain to make it increasingly successful, productive, secure, and amazing. Meanwhile, the biggest blockchain systems, for example, those for advanced monetary standards like bitcoin, are just proceeding to develop.

2 Effects of Blockchain Technology in the Industry

The blockchain is an ever-developing structure of block records connected using cryptography. A blockchain is a disseminated, decentralized, advanced record utilized widely for recording exchanges in numerous PCs. The objective of doing this is to forestall change and control in the resulting blocks. With blockchain, a lot of clients can control how the data record is changed or revised.

Fundamentally, blockchains are comprised of three basic innovations: private key cryptography, P2P network, and program otherwise called the blockchain convention. Blockchain innovation is recognized for considerably affecting a few ventures and segments [16, 17]. Today we are living in a period where there is a noteworthy progression in innovation, and we are looking for arrangements and administrations that improve lives and progressively agreeable. This is the place the blockchain comes into the image. It has been available for quite a while at this point, and a great many individuals and corporates are utilizing this framework in a lot of ways.

Blockchains are utilized in pretty much every industry and business area. Information technology, education, healthcare, retail, digital promoting parts more utilize the blockchain indeed. Interest in the blockchain has been entirely productive. Additionally, the human services segment had a venture of around $0.177 million in the year 2018, and the sum may go up to $0.5.6 million constantly in 2025. With the assistance of blockchains, old frameworks are getting advanced. This has brought about an expansion in proficiency and all the while has chopped down the additional expenses and costs caused in the well-being segment and industry, individually.

Subsequently as indicated by measurements and records, obviously blockchain innovation has a lot of noteworthiness and significance in the change of the whole human services framework positively. It helps the medicinal services industry in various manners, for example, expanded protection, security, expanded effectiveness, creating incorporation, and parts more. Additionally, the blockchains frameworks don't have any focal position, and the exchanges are put away and disseminated over all the systems, individually. Presently, we will view how precisely the blockchains are useful for the human services framework and industry. The blockchain is a progressive revelation and innovation as it causes an organization to comprehend numerous difficulties like the following:

Straightforwardness: With the expanding request in innovation, blockchain offers the perfect measure of straightforwardness to the corporates and different organizations. Consequently, every exchange is recorded and confirmed openly.

Inflexible Nature: This is probably the greatest favorable position of the blockchain. All the information and exchanges recorded can't be adjusted by anyone. This incorporates the framework administrator just as outsiders as well.

Security: In the blockchain innovation, vital information and exchange is utilized broadly over all the frameworks, and it does exclude a concentrated database. This causes an organization to improve its security and make it safe.

Reduced Transaction Expenses: Blockchain takes out the obstruction of outsiders. Banks are additionally not permitted to work the equivalent, and in this way, they have shared exchanges.

These aid in the decrease in expenses indeed.

Advancement: There is an extraordinary space for development and imagination with blockchains. With this innovation, organizations can develop models and contend effectively with different organizations.

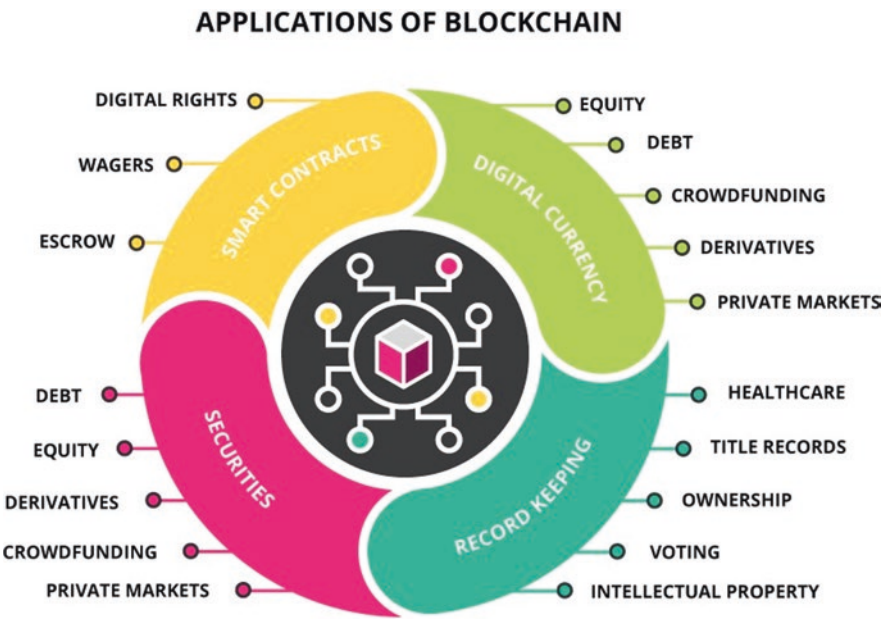


Fig. 1 Blockchain industry applications

3 Blockchain Technology Industry Applications

Blockchain could have veritable end products for the possible destiny of the commercial. Since accounting to exercises, the creating accord midst trade inventors is that it's most likely standard to influence each huge domain of exertion – and the change is presently starting.

Blockchain is an advancement that grants clients and associations to finish trades, and without chatting with a central authority depended on shielding the trade or encrypting the data. By cataloging these trades, it gives honesty of what's going on all through the whole presence of trades and makes these trades progressively secure [18, 19] (Fig. 1).

This innovation is permitting trendsetters and disruptors to turn the tables on a run of the mill business forms in various energizing manners. A portion of the hierarchical impacts of blockchain include the following:

Graceful Chain Following

Blockchain and business go connected at the hip with regard to straightforwardness. Entrepreneurs frequently don't have oversight of who their merchant's providers are; however, innovation could help put this to an end by carrying more receptiveness to the graceful chain. For example, in the food business, it's basic to have solid records that follow each thing to its source if something turns out severely. Thusly, Walmart uses blockchain to screen their produce, where it started from, where it

was arranged and taken care of, and what its expiry date is. Unilever and Nestle furthermore utilize blockchain for tantamount determined following.

Carrying straightforwardness into the flexible chain additionally helps in checking things like the realness of parts and moral sourcing. By saddling this innovation, an organization can likewise give carefully lasting, auditable records for partners and investors [4].

Bringing Down Working Costs

Blockchain grants associations to send and get portions through a programmed game plan of rules called "astute contracts." These take expensive traders, escrow authorities, and former cash-associated arbiters out of the situation.

Splendid understandings are self-executing PC series that can finish the subtleties of an understanding as spread out by their producer. They approve this concurrence with cryptographic code, making it unbreakable as the subtleties of the understanding are normally actioned.

As all exercises related to a particular sharp understanding are direct and recorded, this could moreover diminish the cost of following and bargain. This is promising for overall undertakings as crucial administrative limits like account administrators could be executed immaculately across different countries. Asset confirmation, according to Cybersecurity Ventures, cybercrime harm costs are anticipated to hit $6 trillion every year by 2021. In any case, blockchain could carry some help to this. Since blockchain exchanges aren't limited by a brought together capacity framework and can't be messed with or changed reflectively, they're seemingly more secure than the current frameworks setup. Blockchains store information utilizing refined math and programming that decides that are practically inconceivable for assailants to control.

Each block included onto the chain conveys a hard, cryptographic reference to the past block. That reference is a piece of a scientific issue that should be explained to carry the accompanying block into the system and the chain. This makes an exceptionally encoded advanced unique mark called a hash, making it secure and carefully designed.

In case you're an expert engaged with banking, agreements, settlements, or any piece of the business that includes adjusting as an outsider to an exchange, your job might be influenced by the expanding reception of blockchain. With this sort of innovation, cryptology replaces outsider middle people as the manager of the trust. By utilizing science rather than go-betweens, it can help lessen overhead expenses for organizations or people when exchanging resources or can rapidly demonstrate proprietorship or creation of data.

Giving additional opportunities, blockchain might be the spine that permits digital money exchanges to happen; however, Bitcoin and Ethereum are only the beginnings of what could be conceivable later on. As indicated by Dr. Michael Yuan, Chief Scientist of CyberMiles, an essential blockchain intended for business applications, "Future utilization of this innovation [could include] online business commercial centers and applications, shared fund and protection exchanges, content appropriation, social insurance information trades, B2B bookkeeping applications,

flexibly chain, and client assistance applications." It's an exciting modern lifestyle for organizations that are happy to grasp it. For early adopters and evangelists, the effect of blockchain is restricted uniquely by the creative mind and exertion of the visionaries who will utilize it to change their associations.

4 Significance of Blockchain Technology and Decentralization in Industry

When Bitcoin, the world's first colossal push money, was made in 2009, it was needed to totally subvert the unified establishments which control the budgetary structure. All through late years, this thought of decentralization has been applied not solely to overall bits, at any rate to a gigantic get-together of various uses, from data social affair to deftly chain the chiefs, media, and beguilement and everything within.

As the jobs of blockchain increase, so too does the proportion of foundations attempting to utilize the progression for their optimal position, while holding regards in opposition to the organized push toward decentralization and democratization. This delivers a colossal risk to the primary theory behind the decentralized blockchain.

The original case for decentralization, Bitcoin was made with the conviction that entrusting cash-related trades to hardened pariahs is a clashing and persuading technique for making parcels. This drove Bitcoin's course of action as such electronic cash which would consider speedy, dissipated part overseeing over a structure ensured about by methods for its constituents. As it is passed on in the Bitcoin whitepaper: "A mutual assortment of electronic cash would allow online sections to be sent beginning with one assembling then onto the going with or without encountering a money-related establishment."

This idea changed into the clarification of decentralization over a collection of use cases and attempts, in which it is possible to have "a structure for electronic trades without relying on trust." However, this essential of square chain progression, while fundamental to its flourishing, is in chance as monstrous affiliations try to skip on the square chain train. Inefficient parts of blockchain in industry, for example, the utilization of blockchain development to deftly chain the administrators. Walmart is starting now to apply square chain to follow produce back to its source in basic seconds, yet in the event that associations, for instance, Walmart and Costco, make their concentrated square chains, each coordination provider and supplier on the way should fuse with each and every one of these private square ties to work with these associations. This system will introduce new costs and inefficient perspectives. Nevertheless, if suppliers, collaborations providers, and customers were to all utilize a decentralized square chain answer for managing smoothly chain data and structure, it would be an epic accomplishment for the business by and large.

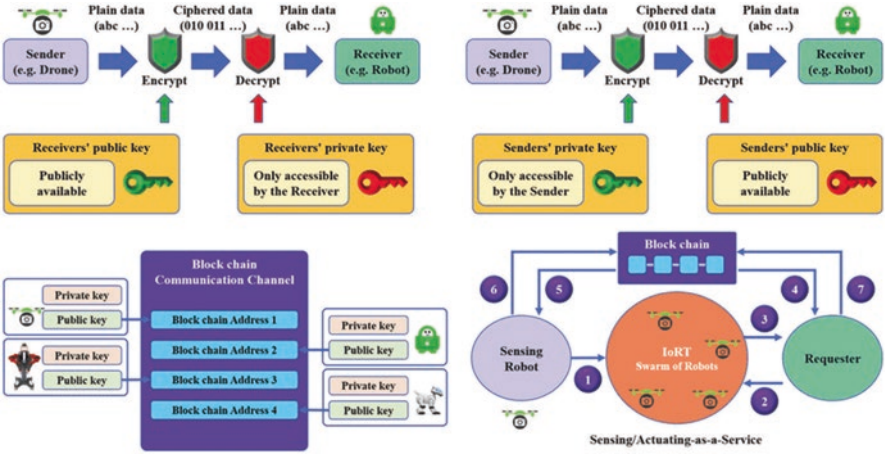


Fig. 2 Centralization of blockchain in industry

The maker of Bitcoin likewise observed that its lethargic breaking point and security depend upon the decentralized idea of its structure. The fundamental security issue of the Bitcoin application is twofold spending, for example, parties attempting to encounter the equivalent impelled money simultaneously on various occasions with no other individual creation feeling of it. The Bitcoin calls attention to that in this structure, "the fundamental inclinations are lost if an acknowledged untouchable is so far required to forestall twofold spending." (Fig. 2)

Private block chains have a vocation in the more unique budget, as attempts can consume this development to recover inward viability. In any case, to tout any private, concentrated blockchain adventure as a dynamic strategy for cooperating is to misrepresent the extent of its rational application. Private block chains are, generally, approval databases that don't give the extra estimation of their open accomplices.

Andreas Antonopoulos, the producer of "Acing Bitcoin," notes, "on the off chance that you take a consent record and express, that is all enchanting, we like the database some piece of it, would we have the decision to have it without the open decentralized P2P [peer-to-peer] open source noncontrolled passed on nature of it, well you just hurled out the youngster with the bathwater." Centralization of movement is unappealing for pariah providers of substance, applications, and affiliations, who become rapidly and totally committed to the holder to the concentrated unforeseen development. Low changing examples of this in the media and news sources are the Apple iTunes store and Spotify, where music providers have no state or authority over their music or what they get in a parcel. Thus, the market is made out of one controlling section, and not just the providers.

Decentralization of movement grants changes and progression to happen considering all out comprehension, and not on the drive of a bound together storing up. One such idea, the "consortium blockchain," is joined around a great deal of partners (around 10–15 individuals or more) rather than a lone controlling substance. Thusly, power is streamed away from a singular fragment while starting not very far

Table 1 Comparison of different blockchain usage in industry

	Public blockchains	Consortium blockchains	Private blockchains
Centralized/ decentralized	Decentralized	Multi-centralized	Decentralized
Participants	Open	A specific group of people who agree to enter an alliance	The central controller decides members that can participate
Credit mechanism	Proof of work	Collective endorsement	Self-endorsement
Bookkeeper	All participants	Participants decide in negotiation	Self-determined
Incentive mechanism	Needed	Optional	Not needed
Prominent advantage	Self-established credit	Efficiency and cost optimization	Transparency and traceability
Typical application scenario	Bitcoin	Clearing	Audits
Load capacity	3–20 times per second	1000–10,000 times/ second	

in the past, giving the limit and security which are key phenomenal position networks for blockchain improvement. A consortium blockchain can be thought of as an open blockchain with obliged assents, or then again, a private blockchain with a trade check gets the opportunity to access various parts.

Ethereum originator Vitalik Buterin includes how consortium square chains could be significant. “A consortium blockchain is a blockchain where the understanding strategy is obliged by a prepicked set of center centers; for example, one may imagine a consortium of 15 cash related establishments, all of which works an inside and of which 10 must sign each square all together for the square to be authentic.” (Table 1)

One theoretical occurrence of an association block chain would be the cohesive nations, which could use an association blockchain for tossing surveying structure purposes, permitting each tending to a nation to be a confirming focus point on the system. This would give a structure wherein each sharing nation gives regulating rules to the system, in any case doesn’t open the system absolutely to the general people.

Buterin states the going as a cause behind the huge capacity of open, dispersed block chains: “This worth distorts an extensive unit in the ethical excellences that cohorts of open block chains have been evolving from the beginning, among the head of which are opportunity, lack of bias, and transparency.”

Although enterprises setting up private block chains might give rise to worry, there is no motivation behind why their model can’t change later on. A venture has the alternative to inevitably open its private block chain to open hubs, in this manner democratizing a formerly concentrated and private system. Regardless of whether

endeavors start through a secretive chain structure, there is an opportunity they might in conversion of time to a progressively open structure.

5 Use of Blockchain in Industry

Blockchain development is shy of the "peak of expanding wants" for the most rising advances. An extent of adventures including social protection, deftly chains the administrators, cash, insurance, and collaborations are occurrences of blockchain. Blockchain is an imitated model which has the critical nature of keeping up a fixed transactions passed on modernized record of trades that are revived subject to framework, and inside substances. In the blockchain, entirely the exchanges or industrialized occasions are logged in as open records available to every single community point in the structure, thus keeping up the fairness of information over the system. The information and data once moved to the structure can never be changed or cleared without comprehension. It at long last compromises a democratized framework that can subsidize in refining the economy. One of the most effective uses of blockchain in organizations is a PC suite known as brilliant comprehension, presented in 1994 by Nick Szabo, which accordingly effects subject to the predefined plan to satisfy different expressions of the comprehension.

Ethereum and Codius have executed wonderful understanding close by blockchain (Table 2).

Traveling should be comfortable, cost-effective, and, most importantly, enjoyable. While charges, booking anomalies, terrible audits, and long queues might be suggestive of the current travel condition, blockchain is stirring things up with a large group of new administrations intended to modernize and smooth out the movement experience. On account of the arrangement of progressively impartial biological systems developed to decrease the nearness of go-betweens, voyagers and specialist organizations can manufacture all the more commonly satisfying connections that add to better finish.

Placing assets into cryptographic types of cash and initial coin offerings ("ICOs") is especially hazardous and hypothetical or the writer to place assets into advanced monetary standards or ICOs. Since each individual's condition is fascinating, a

Table 2 Use of blockchain technology in industry

Name of the industry	Use of blockchain
Winding Tree	Transferring virtual booking hubs
Cool Cousin	Acquisition of superior supervision
Webjet	Tally assurances and eluding imprecisions
Sand block	Refining constancy's fungibility
Accenture	Motivated toward tinier outlines
TravelChain	Constructing the supreme of data

confirmed capable should reliably be guided before choosing any cash-related decisions. Adventures make no depictions or certifications for the accuracy or advantageous quality of the information contained in this. As of date this article was formed, the essayist claims computerized cash.

6 Conclusion

The utilization of blockchain innovation isn't constrained distinctly to any industry. It has a phenomenal future in various areas, for example, flexibly chain the board, advanced publicizing, anticipating, cybersecurity, Internet of things, organizing, and so forth. Blockchain innovation likewise has an enormous imminent to give new openings to occupation in the business. It likewise improves the expert's ability to update themselves. With the assistance of blockchain innovation, it is conceivable to change the entire world into a lot of littler spot. The value-based exercises can be performed a lot quicker and productively utilizing blockchain. Blockchain innovation will be utilized in a lot more divisions later on, for example, in government frameworks as these frameworks are moderate, thick, and prone to defilement. Executing blockchain innovation in government frameworks can make their tasks considerably more secure and effective.

References

1. P. Mell, T. Grance, The NIST definition of cloud computing. Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. Special Publication, pp. 800–145 (2011)
2. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf, NIST cloud computing reference architecture. NIST Special Publicat. **500**(211), pp. 1–28 (2011)
3. M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, A view of cloud computing. Commun. ACM **53**(4), pp. 50–58 (2010)
4. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin Organization, 1–13 2008
5. J. Singh, J.D. Michels, Blockchain as a Service (BaaS): providers and trust. *Proceedings of the IEEE European Symposium on Security and Privacy Workshops*, pp. 67–74, UK, April 2018
6. B.C. Florea, Blockchain and Internet of Things data provider for smart applications. *Proceedings of the 7th Mediterranean Conference on Embedded Computing*, pp. 1–4, Montenegro, June 2018
7. J.H. Park, J.H. Park, Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry **9**(164), pp. 1–13 (2017)
8. T. Salman, M. Zolanvari, A. Abad, R. Jain, M. Samaka, Security services using Blockchains: a state of the art survey. IEEE Commun. Surv. Tutor. **21**(1), 858–880 (2019)
9. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 468–477, Spain, May 2017

10. R.S.M. Lakshmi Patibandla, N. Veeranjaneyulu, A SimRank based ensemble method for resolving challenges of partition clustering methods. J. Sci. Ind. Res. **79**, 323–327 (2020)
11. Y. Niu, L. Wei, C. Zhang, J. Liu, Y. Fang, An anonymous and accountable authentication scheme for Wi-Fi hotspot access with the bitcoin blockchain. *Proceedings of the IEEE/CIC International Conference on Communications in China*, pp.1–6, China, Oct. 2017
12. M.K.R. Ingole, M.S. Yamde, Blockchain technology in cloud computing: A systematic review, International Research Journal of Engineering and Tech, **5**(4), 1918–1921 (2018)
13. R.S.M.L. Patibandla, N. Veeranjaneyulu, Survey on clustering algorithms for unstructured data, in *Intelligent Engineering Informatics. Advances in Intelligent Systems and Computing*, ed. by V. Bhateja, C. Coello Coello, S. Satapathy, P. Pattnaik, vol. 695, (Springer, Singapore, 2018)
14. R.S.M.L. Patibandla, N. Veeranjaneyulu, Performance analysis of partition and evolutionary clustering methods on various cluster validation criteria. Arab. J. Sci. Eng. **43**, 4379–4390 (2018)
15. Z. Zheng, S. Xie, H.N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
16. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
17. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, pp. 181–195, (2020) https://doi.org/10.1002/9781119621201.ch10
18. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle. *In Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, pp. 165–177. https://doi.org/10.4018/978-1-7998-3295-9.ch010
19. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. *Blockchain, Big Data and Machine Learning: Trends and Applications*, 97 (2020)

Review of Blockchain Forensics Challenges

Victor R. Kebande, Richard A. Ikuesan, and Nickson M. Karie

Abstract Blockchain technology has in many ways shown a promising technology where trust can be created between parties. With blockchain, trusted parties can easily transact or exchange information over a cryptographically secured distributed environment. However, based on the blockchain architecture, conducting digital forensic processes faces several problems and challenges. This chapter, therefore, explores the key open problems and challenges experienced while conducting digital forensic processes in blockchain technologies. The authors have leveraged design science research (DSR) to achieve the objectives of this study. Furthermore, the authors have also proposed high-level solutions to the identified problems and challenges.

Keywords Blockchain · Digital forensics · Challenges

1 Introduction

Extraordinary and rapid revolutions in information and communication technology (ICT) in the twenty-first century have seen sporadic inventions and innovations. With these advances in technology, there has been a shift in how digital technologies operate. Notably, computing and processing power together with speed has also shifted and brought about the effectiveness of how businesses are being conducted. One key aspect that has also been the driving force of all these revolutions has been

V. R. Kebande (✉)
Luleå University of Technology, Luleå, Norrbotten, Sweden
e-mail: victor.kebande@ltu.se

R. A. Ikuesan
Community College Qatar, Doha, Qatar
e-mail: richard.ikuesan@ccq.edu.qa

N. M. Karie
Edith Cowan University, Joondalup, WA, Australia
e-mail: nkarie@ecu.edu.au

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_3

the Internet. The Internet has brought about technology-centric inventions and transformation which has also played a role in how business transactions are conducted [1].

The result of these transformations has been the exchange of digital information in a very effective manner. Information has become a very valuable asset, which in most cases has been the main product that many businesses have had to focus on. The exchange of information has meant that several technologies solely rely on information to thrive in their trust-based businesses. One important technology that has been embraced as a result of the rapid revolutions has been blockchain technology. This relatively new technology is able to use distributed ledger technology to support digitized economies. The International Data Corporation (IDC) has projected that by 2021, a majority of data from different sources will be registered in a public blockchain [62, 63]. Furthermore, a number of blockchain distributed ledgers will be incorporated in the Internet of Things (IoT) sensors. This provides a very important aspect, which allows blockchain technology to be interconnected on different business networks, ledgers, and other industrial ecosystems.

While the benefits of blockchain look promising, the blockchain data-centric paradigm is bound to be affected by a number of problems and challenges like cyberattacks, cyber threats, and other digital crimes. Therefore, as blockchain-based businesses keep expanding, there is a need to conduct digital forensic processes across the different blockchain-based consortium. Digital forensics presents the most acceptable approaches to prove attribution and also be able to build a forensic-based hypothesis. However, there still exist a number of challenges when trying to apply forensic processes in blockchain architectures. The chapter has been presented in three folds: first, the author uses design science research (DSR) to identify potential literature; second, blockchain forensic models are identified from which challenges are extracted; and third, a proposal for high-level solutions is given. In the later section, future challenges are also identified.

The remainder of the chapter is structured as follows. Section 2 handles Background, while Sect. 3 explains the Related Work. This is followed by Research Methodology in Sect.. 4 and identified Blockchain Forensic Investigation Models in Sect. 5. Results and Discussions are given in Sect. 6, Future Challenges in Sect. 7, and Conclusion is given in Sect. 8.

2 Background

2.1 Blockchain Structure

Blockchain allows data to be shared among trusted peers. Through blockchain, transactions and decentralized data can easily be propagated among unreliable blockchain participants based on the transactions among the distributed peers. Moreover, this technology can apply a data structure, which contains a list of blocks that are able to record generated cryptographic hash values for a transaction that has

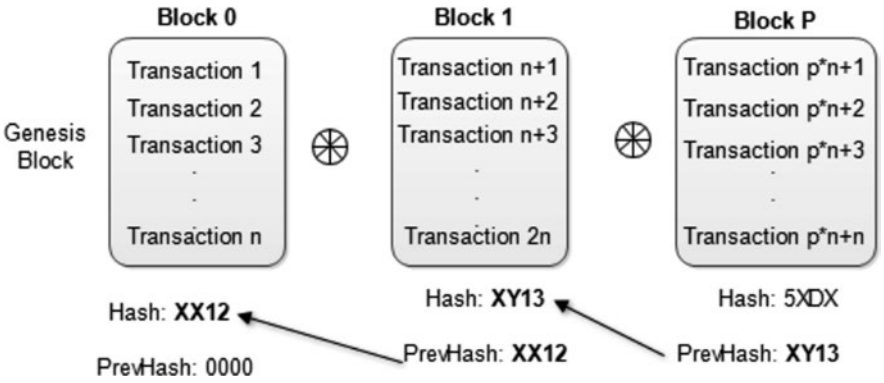


Fig. 1 Blockchain pipeline

been completed and done in a given order. A chain of the hashes created from the transactions forms a distributed peer-to-peer (P2P) blockchain that is tamper-proof as is shown in Fig. 1.

Figure 1 shows a simple blockchain connection structure having blocks 0, 1, up to P. Each block has data that is represented as a transaction, a freshly generated hash, and the hash of previous blocks. The genesis block which is labeled as the genesis block does not have a previous hash since it is the block that starts the chain. Generally, blockchain allows the timestamping of a document to eliminate backdating [2, 3]. Cryptographic hashes are used to uniquely identify the contents of a block to prevent alteration of modification. To protect the structure, proof of work is used that limits the change of the contents of the block [64, 65].

2.2 Digital Forensic Science

Digital forensics (DF) attempts to use scientifically proven methods or techniques to excavate digital artifacts from computing devices. This process can identify, recover, and investigate a digital crime through the presentation of facts and findings through evidence presentation processes. Following the formalization of DF as a science at the 2001 Digital Forensics Research Workshop (DFRWS), in Utica, NY [4], several definitions have been adapted over the years to include a generic definition of digital forensics [5], context-specific definitions [6–10], and component-specific definition such as sub-domains [11–13]. Relying on these formalism, DF is the use of "scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources to facilitate or further the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." From its inception, several digital forensic process models have been proposed by different researchers and

research groups [14]. However, [15] has presented it as an investigative technique that uses a prescribed technique with the main aim of creating a forensic hypothesis that can be used for litigation purposes. The next section thus presents some general concepts of the digital forensic investigation process.

2.3 Digital Forensic Investigation Process

A number of digital investigation processes have been proposed, and there exist variations on the processes; however, in the context of this research, the authors take a generic perspective of the investigation processes. Consequently, the authors also explore some useful investigation processes. A multitiered hierarchical, objective-based digital forensic investigation process model [16] gave a comprehensive view of how investigation processes can be conducted. Notably, [17] has also proposed a novel forensic investigation process for the cloud that focused on proactive forensics. Besides, [18] have also proposed a harmonized digital forensic investigation process model that incorporates several processes. Nevertheless, [19] has proposed a process model that includes the following processes: identification, collection, preservation, transportation, storage, analysis, interpretation, attribution, reconstruction, presentation, and destruction.

Lastly, [20] highlighted key characteristics for an investigation process as follows: practical and general to the technology, not be constrained to current products and procedures. Besides, this model must be specific enough that general technology requirements for each process can be developed. The model must be abstract and apply to law enforcement investigations, corporate investigations, and incident response. Having looked at various contributions by a number of researchers, the authors have adopted the investigation processes that were defined during DFRWS shown in Fig. 2.

While other applicable models can be considered, this study assumes that the complexity of blockchain itself can complicate the potential forensic processes; hence, simpler/linear forensic process models capable of providing the basic underlying functionalities of forensic science should be used. Figure 2 shows the processes of investigations based on DFRWS, which begins with potential artifact identification and ends when the investigation has been presented.

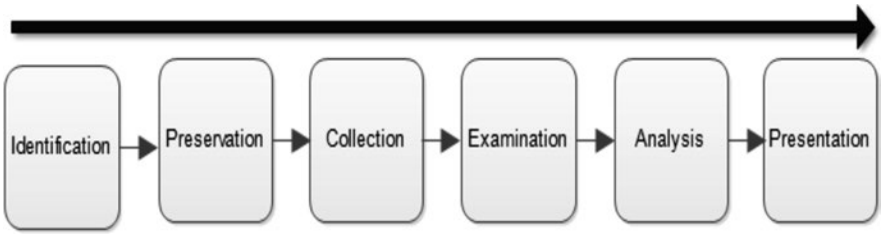


Fig. 2 Digital forensic investigation process

3 Related Works

Quite a good number of researches on blockchain technologies exist. In this chapter, however, focus is given to blockchain studies that attempt to develop a forensic process model which can be leveraged for digital investigation. Research conducted by [21] explored a number of security and privacy consumption and trading data where the authors were able to highlight serious security challenges. Furthermore, research by [22] showed that, based on how the cloud is distributed, there is unavailability of trustworthy records in conducting blockchain forensics which further points to the hypothesis that there is a potential research gap in blockchain-based digital forensic processes: an investigative challenge.

Additionally, [22] explored the pros and cons of using blockchain/bitcoin cryptocurrency approach in order to see if the underlying blockchain technology could be used in addressing forensic investigation approaches in the cloud. The authors defined the research as an approach that assesses cryptocurrency risks on blockchain. Other relevant work by [23] gave consideration for blockchain security challenges and explored settlement of blockchain, security of the transactions, security of the wallet, and the security of the software; while this has some importance, the forensic approach has been rarely explored. Research by [24] presented a survey on blockchain-based approaches for several security services. The authors argue that blockchain is a secured and distributed ledger that can help resolve many of the problems with centralization. Their main objective, however, was centered on giving insights on the use of security services for current applications and highlight the state-of-the-art techniques that are currently used to provide different services, to describe their challenges, and to discuss how the blockchain technology can resolve these challenges. More research by [25] presented the challenges and solutions on blockchain in the Internet of Things. In their chapter, the authors proposed an architecture that is hierarchical and consists of smart homes, an overlay network and cloud storage coordinating data transactions with blockchain to provide privacy and security. Their work [25] did not focus on blockchain forensics as is the case of this chapter. Other research that are pertinent and have contributed in evidence extraction strategies that could be leveraged in the case of blockchain include [26–30].

While the abovementioned research studies remain useful and insightful, none of these studies was focused on blockchain forensics: open problems, challenges, and a proposal toward a high-level solutions as presented in this chapter. However, the study highly acknowledges the contribution made by the abovementioned authors. To fully address the observed limitation, and providing a verifiable approach toward the proposed high-level solution and the identification of blockchain forensic challenges, the methodology described in the next section is utilized.

4 Research Methodology

Studies in [11, 31] have explored the process of utilizing design science research (DSR) as an effective approach toward conducting a systematic review within the context of digital forensics. The design science methodology has been shown to provide a verifiable and repeated process for conducting an exploratory study [31]. This approach is further adapted in this study. The adapted process comprises three distinct phases, as shown in Fig. 3. The first phase feeds into the second, while the second feeds into the third, as further described in the proceeding subsections [66, 67].

4.1 Phase I

This phase deals with the process of formulating the research direction for the literature review process. To formulate the research questions, an initial exploratory study was conducted using Google Scholar search engine (which generated a total of 7870 output) to ascertain the extent of digital forensics-related research in the blockchain domain. Based on the preliminary observation, the following research questions were crafted:

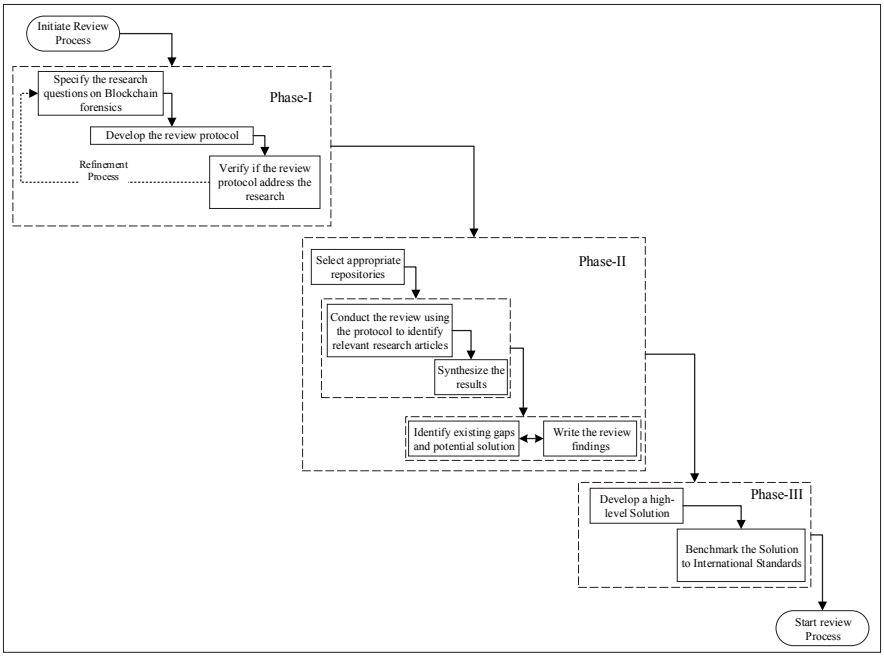


Fig. 3 Review methodology

1. What are the existing forensic models for investigating blockchain-related incident?
2. Are there standardized forensic processes for blockchain-related incidents?
3. What are some fundamental limitations of conducting a forensic investigation in a blockchain environment?

As highlighted in the Phase I of Fig. 3, to address these research questions, a formalized review is required. However, from the prior preliminary investigation, most research conducted within the domain of digital forensics and blockchain technology is found within the IEEE Xplore, ScienceDirect, SpringerLink, and ACM digital repositories. This observation was achieved after a further date-based filtration from 2015 to 2020, of the preliminary search. A total of 7280 results was generated, using the keyword "blockchain forensics." This keyword was ascertained to provide requisite search coverage for the three research questions. Therefore, the protocol was considered satisfactory for this study. The review protocol adapted for this study is further itemized thus:

1. Extract keywords from the research questions.
2. Enumerate filtration methods.
    - Filter by exact match using double quotes (" ")
    - Filter by date range (2015 to 2020 in this case)
    - Filter by title relevance
    - Filter based on the relevance of the abstract
    - Filter by coherence between the research gap identified in the manuscript and the result obtained, where applicable
3. Identify the relevant digital repositories.
    - ACM, IEEE Xplore, ScienceDirect, and SpringerLink repositories (in this case)
4. Enumerate method of combining keywords.
    - The use of \&, \&\&, +, or, intitle, intext, and
5. Select and store appropriate items for review.

Furthermore, the study limits the search space to journal, conference, or book chapter manuscripts. The outcome of this phase is used as input into Phase II as depicted in Fig. 3.

4.2 Phase II

The digital repositories and the review protocol identified in Sect. 4.1 are used as input into this phase. The result of the application of the review protocol is shown in Table 1 and the corresponding literature for each repository. A synopsis of the

Table 1 Output of protocol application

Repository	Observed record	After filtration
ACM	4545 (from 2,842,393) records	1
ScienceDirect	173 records	4
IEEE Xplore	176 records	5
SpringerLink	196 records	4

observed research challenges and limitations is further presented in the subsequent sections. This also includes the identification of the various blockchain-based forensic models, which are somewhat related to blockchain technology.

5 Blockchain Forensic Investigation Models

One of the fundamental requirements of any digital forensic investigation process is the availability of digital evidence. Such evidence can be acquired from different sources based on the specific case under investigation. In the case of blockchain forensics, several digital forensic investigation models have been proposed to help in identifying, preserving, collecting, examining, analyzing, and presenting findings based on a specific application of blockchain technologies. Knowing that blockchain technologies have not been fully integrated into most of the existing digital forensics frameworks, this section samples and briefly explains some of the proposed blockchain forensics models as part of research questions raised in Phase 1 of this chapter (Table 2).

5.1 Forensic-Chain

Proposed by [35, 36], the forensic-chain framework is meant to offer integrity and tamper resistance to the digital forensic-chain of custody. The forensic-chain framework takes advantage of blockchain's capability and combines it with cryptographic hashing and encryption to create documentation about evidence access that is tamper-proof [35, 36], thus maintaining and tracing the digital forensic-chain of custody.

5.2 Block4Forensic

The development of smart and connected vehicles [47] saw the need for forensic analysis and proposed Block4Forensic, which is an integrated lightweight blockchain framework for forensics applications of connected vehicles. This framework

Table 2 Summary of the selected literature

Repository	Reference	Title of manuscript
ACM	[32]	Weighted forensics evidence using blockchain
ScienceDirect	[33–36]	A blockchain-based solution for the custody of digital files in forensic medicine Blockchain-based photo forensics with permissible transformations Forensic-chain: Blockchain-based digital forensics chain of custody with PoC in Hyperledger Composer Blockchain-based forensic system for collection and preservation of network service pieces of evidence
IEEE Xplore	[37–41]	Blockchain evolution: From bitcoin to forensic in smart grids BIFF: A blockchain-based IoT forensics framework with identity privacy B-FICA: Blockchain-based framework for auto-insurance claim and adjudication Unravelling Ariadne's thread: Exploring the threats of decentralized DNS A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues
SpringerLink	[42–45]	SoK: Transparent dishonesty – front-running attacks on blockchain Design of real-time transaction monitoring system for blockchain abnormality detection Blockchain in context Big data and blockchain

was intended to facilitate trustless, traceable, and privacy-aware post-accident analysis with minimal storage and processing overhead [47].

5.3 Bitcoin Transaction Network Analytic Method

The rising use of cryptocurrencies like Bitcoin has also seen an increase in its malicious use to launder money on the dark Web. As a way to trace and analyze suspected Bitcoin transactions and addresses, [48] proposed a Bitcoin transaction network analytic method for use in blockchain forensic investigations. The goal of [48] was to provide a reliable forensic investigation model which can also be beneficial to financial security.

5.4 SDNLog-Foren

In another effort, [49] wanted to provide a way to secure log files with fine-grained access control in proper storage without any modification. To achieve this objective, [49] proposed SDNLog-Foren: a blockchain-based approach to improve the security of log management in SDN for network forensics. Several experiments were

conducted to evaluate SDNLog-Foren to prove that it can help organizations securely keep sensitive network log data regardless of any compromise at some different components of the SDN.

5.5 BlockSLaaS

Leveraging on the immutable property of blockchain technology, [50] proposed BlockSLaaS: a forensic-aware blockchain-assisted secure logging-as-a-service for a cloud environment. The goal was to help securely store and process logs by tackling the multi-stakeholder collusion problem and ensuring integrity and confidentiality [50].

5.6 FIF-IoT

In their proposal, [51] argues that the increased deployment of Internet of Things (IoT) devices makes them a lucrative target for cyberattacks and potential tools for committing cybercrimes. To counter these vices, [51] proposed FIF-IoT: a forensic investigation framework that uses blockchain technology to find facts in criminal incidents in IoT-based systems.

5.7 BIFF

With the rising attacks in IoT environments, [38] take advantage of existing blockchain technologies and propose a blockchain-based IoT forensics framework. The framework is meant to enhance the integrity, authenticity, and non-repudiation properties of any collected evidence. According to [38], BIFF was also meant to "record events of the entire life cycle of digital evidence in a transparent, traceable, and identity privacy-preserving way."

5.8 B-FICA

B-FICA was proposed by [39] for auto-insurance claims and adjudication for connected and automated vehicles (CAVs). The idea was to be able to track both sensor data and entity interactions with two-sided verification. In addition, B-FICA was designed to facilitate the collection of relevant evidence from potential liable entities.

5.9 B-CoC

In an effort to try and improve on the manual chain of custody (CoC), [52] proposed B-CoC, a framework meant to dematerialize the CoC process. The study aimed to guarantee auditable integrity of digital pieces of evidence and traceability of owners. Their research was backed up by the fact that most digital evidence CoC was manually managed with anyone involved in the chain required to fill in documents accompanying the evidence.

6 Results and Discussions

This chapter presents different problems and challenges in relation to blockchain forensics as a contribution in the digital forensic domain. Using Table 3, the authors have also presented a proposal for high-level solutions for each challenge. Each of the challenges that has been presented has also been mapped to relevant and respective literature. The scope of the chapter is defined by the different challenges identified in Table 3. The identified challenges provide an answer to the third research question posited in Subsection 4.1. These fundamental limitations of conducting a forensic investigation in a blockchain environment addressed this research question. The challenges are further explained in terms of their scope, and a corresponding high-level solution is proposed.

Most of the challenges identified in this chapter, however, were selected as common examples to facilitate this study and do not by any means constitute an exhaustive list. The identified problems and challenges can be used in the digital forensic domain, for example, to explicitly describe processes and procedures that focus on addressing the individual challenges. Moreover, the identified problems and challenges in this chapter can also help present new research opportunities for the researchers to find specific solutions to the identified challenges. Developers of blockchain technologies can, further, use the identified challenges to fine-tune their systems to mitigate as many challenges as possible.

Given that blockchain is a ledger that is shared, the data that is shared among peers in most cases may be immense, and it is bound to grow as a result of constant communication [47]. It is important to mention that data that is required for purposes of forensics is not contained in a shared ledger per se; this is owing to the fact that sharing these data may impede forensic investigations or may hamper investigation processes if a potential incident could occur. In this approach, we utilized design science research (DSR) as a way of identifying pertinent potential blockchain forensic challenges, with a total of 7870 output articles, but after the exclusion criteria that are mentioned in Table 1, we identified 13 essential articles that helped in the formulation of our arguments. In the view of these foregoing, we were able to identify investigative models aligned to blockchain technology [39, 39, 47–49, 51, 52] and potential challenges and a mention of high-level solutions.

Table 3 High-level solutions for the open problems

Open problem	Description	High-level solution
CPU energy theft	Malicious intruders have changed the attack approaches. It is possible to steal the computing power, and then they use the computing power to trade with the virtual currency which is then exchanged for cash	Use intrusion-based malware-like tools. This involves collecting existing malware attack signatures and being able to insert the signatures in a non-malicious fashion. The inserted malware should act as decoys that collect infesting malware for digital forensic purposes [53–55]
Collision attack	These attacks can be realized when a malicious intruder easily explores different strings in a blockchain environment that can easily hash to the same value. According to [2], a cyberattacker can easily generate the same address with two different public keys	Enforce a proactive forensic-based approach that can collect data, and send it to a centralized location for forensic analysis or reactive approaches [56]
DDoS attack	A huge amount of unenforceable data/traffic can be flooded by an attacker, thus affecting several nodes in a given network	Forensic investigation on DDoS should rely on the fact that network forensic pieces of evidence are properly captured and preserved before investigation
Duplicated signatures	Normally signatures can be duplicated in an unrealistic fashion where the attacker can find signatures that are identical in a blockchain nonce. Research by ~\cite{bos2014elliptic} found more than 100 public keys using the same blockchain nonce in more signatures	Forensically investigate multi-signature transaction parties and ensure the number of signatures involved in the transactions matches the number of public keys being used
RPC eavesdropping	An attacker can easily listen to messages being passed by peers over the nodes by trying to decrypt messages using private keys	Investigate anonymous identities involved in proof of work, and excavate the hidden non-content data
Code vulnerabilities	An attacker can easily exploit a number of vulnerabilities in order to either create a public or private key in order to hijack sessions or blockchain transactions and signatures	Forensically investigate vulnerable points like OpenSSL where public/private key pair can be used to hijack sessions
Man in the middle attack	An attacker can easily eavesdrop over a blockchain transaction infrastructure, and sensitive or critical data can easily be relayed through interception	Proactively collect real-time traffic to be able to profile suspicious adversarial patterns [5]
Malicious code injection	Based on existing vulnerable nodes or points, an attacker can easily inject code that ends up compromising transactions. For example, shell injection, script injection	Use intrusion-based decoys like honeypots to forensically trap malicious code based on the signatures [53–55]

(continued)

Table 3 (continued)

Open problem	Description	High-level solution
Botnet attack	Attackers can be able to create a distributed infrastructure for botnets on the Ethereum network, and easily their target is on blockchain command infrastructure and ability to resist takedown, and this may lead to prolonged damage	Conduct botnet signature analysis and event reconstruction and interception of C&C communications in order to disrupt the botnet through network-level observation [57]
Brute force attack	Infiltrating blockchain transactions is possible when a trader awaits acceptance of the transaction. The attacker can invalidate the blocks in order to make it longer, thus denying the victim time to accept the transactions	Investigate the probabilities of proof of work to explore possible blockchain transaction block collisions
Illegal halting of blockchain transactions	A transaction can easily be halted, and this could happen through the illegal spamming of transactions through illegal stuffing of transactions inside each transaction, hence causing an indefinite response of the transactions	Investigate the blockchain-based content data and source IP in order to detect and profile potential incidents

Our study has explicitly provided diverse avenues that have allowed the identification of blockchain forensics peculiarities. Important to highlight is the fact that blockchain technology adoption in many areas assumes that the channel exists as an immutable ledger and computationally infeasible for a potential attacker; however, given that a majority of systems are mainly subject to compromise, a projection of potential and incident response strategies may act as a salvaging point for what could have gone wrong. Different environments that have the potential of leveraging blockchain exist, like the Internet of Things (IoT) forensics [1, 56, 58, 59]; this is owing to connectivity and heterogeneity of devices and environment and the fact that in some situations intermediaries exist and different unauthorized communication patterns among peers may warrant an investigation. In essence, such an ecosystem may, in some situations, guarantee proper or stronger record-keeping strategies; however, in the context of this chapter, we argue that it may be important to identify the time that an incident may be detected and when an investigation commences. Notably, there still exist varying circumstances, where, for example, parties in a blockchain are bound to share their chain among peers and deliberately a peer may share a wrong chain with the intention of tampering with the created chain. While this cannot succeed in a blockchain, we identify this as a potential anomaly that may be subjected to early anomaly detection, for purposes of building a preliminary investigative hypothesis. It is also important to note that as a result of the investigation conducted and at the time of writing this chapter, there still do not exist any formal or agreed standards on forensically investigating blockchain-based applications.

7 Potential Future Challenges

Blockchain as a technology has gained a lot of interest in diverse areas, and as a result, many areas have seen proliferations in security, privacy, and trust. In response to the first research question posited in Subsection 4.1, the result discussed in Sect. 6 reveals there exist several models. However, there is no specific process model for blockchain forensics. Moreover, there still exist potential blockchain forensic research areas that need to be addressed. We list the following areas which have the potential of being explored:

- Institute blockchain forensic approaches that are based on forensic design techniques [60].This open challenge further answers the second research question on the availability of a standardized forensic process for blockchain incident investigation.
- Research on the integrity of data exists as a factor of communication during the creation of immutable channels.
- The security given that blockchain nodes could have access to database nodes; hence in some situations, this could be a challenge for the decentralized systems [61].
- Investigations on the decentralized data on the nodes during the process of querying transactions [61].
- Research on simulating live forensics in decentralized environments using deep learning and machine learning approaches [6, 30].
- Proposal of standardized techniques/approaches for forensically conducting investigations for blockchain-based applications.

Our study has identified pertinent issues that are regarded as potential future challenges; as a result, in the next section, a conclusion of this study is given.

8 Conclusion

This chapter has explored the general blockchain forensics open problems, challenges, and a proposal of high-level solutions as a contribution to this research study. The authors have highlighted the potential challenges and the possible forensic approaches that can be applied to those processes using design science research (DSR). It is not definite how the evidence in blockchain will lead to the seizure of blockchain-based applications; however, it should be noted that the aforementioned approaches can easily aid forensic experts on how the various challenges can be explored. The findings from this research help researchers to understand the current state of the art and significantly on the future of blockchain-based applications and the prevailing forensic challenges. Future work is aimed at proposing a taxonomy of blockchain-based challenges and mapping them with standardized forensic processes.

References

1. S. Khorashadizadeh, A.R. Ikuesan, V.R. Kebande, Generic 5g infrastructure for IoT ecosystem. In *International Conference of Reliable Information and Communication Technology*, pp. 451–462, Springer, 2019
2. F. Mendel, T. Peyrin, M. Schl ̈affer, L. Wang, S. Wu, Improved cryptanalysis of reduced ripemd-160. In *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 484–503, Springer, 2013
3. J.W. Bos, J.A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow, Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*, pp. 157–175, Springer, 2014
4. P. Gary, A road map for digital forensic research. In *Digital Forensics Research Workshop*, 2001
5. V.R. Kebande, N.M. Karie, R.D. Wario, H. Venter, Forensic profiling of cyber-security adversaries based on incident similarity measures interaction index. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, pp. 1–6, IEEE, 2018
6. V.R. Kebande, R.A. Ikuesan, N.M. Karie, S. Alawadi, K.-K.R. Choo, and A. Al-Dhaqm, Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (eco) in iot environments, forensic Science International: Reports, p. 100122, CFRaaS and Wiley 2020
7. S. Philomin, A. Singh, A. Ikuesan, H. Venter, Digital forensic readiness frame-work for smart homes. In *International Conference on Cyber Warfare and Security*, pp. 627–XVIII, Academic Conferences International Limited, 2020
8. Ikuesan AR, Abd Razak S, Salleh M, Venter HS. Leveraging Human Thinking Style for User Attribution in Digital Forensic Process. International Journal on Advanced Science, Engineering and Information Technology **7**(1):198–206.
9. A.R. Ikuesan, H.S. Venter, Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet? Digit. Investig. **30**, 73–89 (2019)
10. A. Singh, A.R. Ikuesan, H.S. Venter, Digital forensic readiness framework for ransomware investigation. In *International conference on digital forensics and cyber crime*, pp. 91–105, Springer, 2018
11. A. Al-Dhaqm, S. Abd Razak, D.A. Dampier, K.-K.R. Choo, K. Siddique, R.A. Ikuesan, A. Alqarni, V.R. Kebande, Categorization and organization of database forensic investigation processes. IEEE Access **8**, 112846–112858 (2020)
12. I.R. Adeyemi, S. Abd Razak, N.A.N. Azhan, A review of current research in network forensic analysis. Int. J. Digit. Crime Forensics **5**(1), 1–26 (2013)
13. I.R. Adeyemi, Online psychographic model for insider identification. PhD thesis, Universiti Teknologi Malaysia, 2015
14. A. Singh, H.S. Venter, A.R. Ikuesan, Windows registry harnesser for incident response and digital forensic analysis. Aust. J. Forensic Sci. **52**(3), 337–353 (2020)
15. V.R. Kebandeetal, A novel cloud forensic readiness service model. PhD thesis, University of Pretoria, 2018
16. N.L. Beebe, J.G. Clark, A hierarchical, objectives-based framework for the digital investigations process. Digit. Investig. **2**(2), 147–167 (2005)
17. V.R. Kebande, H.S. Venter, On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. Aust. J. Forensic Sci. **50**(2), 209–238 (2018)
18. V.R. Kebande, N.M. Karie, R.A. Ikuesan, H.S. Venter, Ontology-driven perspective of CFRaaS Wiley Interdisciplinary Reviews: Forensic Science, p. e1372 (2020)
19. F. Cohen, J. Lowrie, C. Preston, The state of the science of digital evidence examination. In *IFIP International Conference on Digital Forensics*, pp. 3–21, Springer, 2011
20. B. Carrier, E.H. Spafford, et al., Getting physical with the digital investigation process. Int. J. Digital Evidence **2**(2), 1–20 (2003)

21. N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. **15**(5), 840–852 (2016)
22. Y. Zhang, S. Wu, B. Jin, J. Du, A blockchain-based process provenance for cloud forensics. In *2017 3rd IEEE International Conference on Computer and Communications (ICCC)*, pp. 2470–2473, IEEE, 2017
23. Y. Zhao, B. Duncan, The impact of crypto-currency risks on the use of blockchain for cloud security and privacy. In *2018 International Conference on High Performance Computing & Simulation (HPCS)*, pp. 677–684, IEEE, 2018
24. T. Salman, M. Zolanvari, A. Erbad, R. Jain, M. Samaka, Security services using blockchains: a state of the art survey. IEEE Commun. Surv. Tutor. **21**(1), 858–880 (2018)
25. A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and solutions, arXiv preprint arXiv:1608.05187, 2016
26. V.R. Kebande, N.M. Karie, H. Venter, Cloud-centric framework for isolating big data as forensic evidence from IOT infrastructures. In *2017 1st International Conference on Next Generation Computing Applications (NextComp)*, pp. 54–60, IEEE, 2017
27. S. Li, T. Qin, G. Min, Blockchain-based digital forensics investigation frame-work in the internet of things and social systems. IEEE Trans. Computat. Social Syst. **6**(6), 1433–1441 (2019)
28. D. Billard, B. Bartolomei, Digital forensics and privacy-by-design: example in a blockchain-based dynamic navigation system. In *Annual Privacy Forum*, pp. 151–160, Springer, 2019
29. H. Al-Khateeb, G. Epiphaniou, H. Daly, Blockchain for modern digital forensics: the chain-of-custody as a distributed ledger. In *Blockchain and Clinical Trial*, pp. 149–168, Springer, 2019
30. N.M. Karie, V.R. Kebande, H. Venter, Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Sci. Int. Syner. **1**, 61–67 (2019)
31. A. Al-Dhaqm, S. Razak, K. Siddique, R.A. Ikuesan, V.R. Kebande, Towards the development of an integrated incident response model for database forensic investigation field. IEEE Access, 8(1) (2020)
32. D. Billard, Weighted forensics evidence using blockchain. *ACM International Conference Proceeding Series*, vol. Part F137704, pp. 57–61, 2018
33. M. Lusetti, L. Salsi, A. Dallatana, A blockchain based solution for the custody of digital fi les in forensic medicine. Forensic Sci. Int. Digital Investig. **35**(301017), 1–11 (2020)
34. R. Zou, X. Lv, B. Wang, Blockchain-based photo forensics with permissible transformations. Comput. Security, 87 (2019)
35. A.H. Lone, R.N. Mir, Forensic-chain: Blockchain based digital forensics chain of custody with PoC in hyperledger composer. Digital Investig. **28**, 44–55 (2019)
36. G. Mací a-Fern andez, J.A. G omez-Hern andez, M. Robles, P. Garc ıa-Teodoro, Blockchain-based forensic system for collection and preservation of network service evidences. Digital Investig. **28**, S141 (2019)
37. I. Kotsiuba, A. Velykzhanin, O. Biloborodov, I. Skarga-Bandurova, T. Biloborodova, Y. Yanovich, V. Zhygulin, Blockchain evolution: from bitcoin to forensic in smart grids. *Proceedings – 2018 IEEE International Conference on Big Data, Big Data 2018*, pp. 3100–3106, 2019
38. D.P. Le, H. Meng, L. Su, S.L. Yeo, V. Thing, BIFF: a blockchain-based IoT forensics framework with identity privacy. *IEEE Region 10 Annual International Conference, Proceedings/ TENCON*, vol. 2018-October, no. October, pp. 2372–2377, 2019
39. K. Fan, Y. Ren, Z. Yan, On Blockchain. *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)*, pp. 1349–1354, 2018
40. C. Patsakis, F. Casino, N. Lykousas, V. Katos, Unravelling ariadne's thread: exploring the threats of decentralised DNS. IEEE Access **8**, 118559–118571 (2020)
41. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. **22**(2), 1191–1221 (2020)

42. S. Eskandari, S. Moosavi, J. Clark, Sok: transparent dishonesty: front-running attacks on blockchain. In *International Conference on Financial Cryptography and Data Security*, pp. 170–189, Springer, 2019
43. J. Bang, M.-J. Choi, Design of real-time transaction monitoring system for blockchain abnormality detection. In *International Conference on Applied Physics, System Science and Computers*, pp. 229–234, Springer, 2018
44. A.J. Ehrenberg, J.L. King, Blockchain in context. Inf. Syst. Front. **22**(1), 29–35 (2020)
45. H. Hassani, X. Huang, E.S. Silva, Big data and blockchain. In *Fusing Big Data, Blockchain and Cryptocurrency*, pp. 7–48, Springer, 2019
46. A.H. Lone, R.N. Mir, Forensic-chain: ethereum blockchain based digital forensics chain of custody. Sci. Pract. Cyber Secur. J. Vol 1 (2018)
47. M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun. Mag. **56**(10), 50–57 (2018)
48. Y. Wu, F. Tao, L. Liu, J. Gu, J. Panneerselvam, R. Zhu, M.N. Shahzad, A bitcoin transaction network analytic method for future blockchain forensic investigation. IEEE Trans. Netw. Sci. Eng. (2020)
49. P.T. Duy, H. Do Hoang, N.B. Khanh, V.-H. Pham, et al., Sdnlog-foren: ensuring the integrity and tamper resistance of log files for SDN forensics using blockchain. In *2019 6th NAFOSTED Conference on Information and Computer Science (NICS)*, pp. 416–421, IEEE, 2019
50. S. Rane, A. Dixit, Blockslaas: blockchain assisted secure logging-as-a-service for cloud forensics. In *International Conference on Security & Privacy*, pp. 77–88, Springer, 2019
51. M. Hossain, Y. Karim, R. Hasan, Fif-iot: a forensic investigation framework for iot using a public digital ledger. In *2018 IEEE International Congress on Internet of Things (ICIOT)*, pp. 33–40, IEEE, 2018
52. S. Bonomi, M. Casini, C. Ciccotelli, B-coc: a blockchain-based chain of custody for evidences management in digital forensics, arXiv preprintarXiv:1807.10359, 2018
53. M. Brand, C. Valli, A. Woodward, "A threat to cyber resilience: a malware rebirthing botnet," 2011
54. V.R. Kebande, H.S. Venter, A cloud forensic readiness model using a botnet as a service. In *The International Conference on Digital Security and Forensics (Dig-italSec2014)*, pp. 23–32, Ostrava: The Society of Digital Information and Wireless Communication, 2014
55. R. Gummadi, H. Balakrishnan, P. Maniatis, S. Ratnasamy, Not-a-bot: improving service availability in the face of botnet attacks. In NSDI **9**, 307–320 (2009)
56. V.R. Kebande, I. Ray, "A generic digital forensic investigation framework for internet of things (IoT)," In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 356–362, IEEE, 2016
57. B. Cusack, Botnet forensic investigation techniques and cost evaluation, 2014
58. V.R. Kebande, N.M. Karie, H.S. Venter, Adding digital forensic readiness as a security component to the IoT domain, 2018
59. V.R. Kebande, S. Malapane, N.M. Karie, H. Venter, R.D. Wario, Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. In *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 93–98, IEEE, 2018
60. N.H. Ab Rahman, W.B. Glisson, Y. Yang, K.-K.R. Choo, Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput. **3**(1), 50–59 (2016)
61. J. Bao, D. He, M. Luo, K.-K.R. Choo, A survey of blockchain applications in the energy sector. IEEE Syst. J. Vol 1 (2020)
62. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications*. Taylor & Francis, UK (CRC Press, 2020)
63. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. Blockchain, Big Data and Machine Learning: Trends and Applications, 97 (2020)
64. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, 2020), pp. 1–23

65. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global), IGI-Global, USA. pp. 165–177
66. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
67. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), Wiley USA. pp. 181–195

Distributed Computing in Blockchain Technology

Vijay Ramalingam, Dineshbabu Mariappan, S. Premkumar, and C. Ramesh Kumar

Abstract Appropriated computing in blockchain technology distributed innovation stage for creating decentralized applications and information stockpiling. A disseminated record is database that is con exotically shared and inner associated with arrange hubs. It permits exchanges data and to have open record database in the executive framework. The ledger can be described as a ledger of any transactions or contracts kept up in decentralized form across different geolocation connection which are made up with network nodes. The contestant at each node of the network can access the registered data shared across that network and can own an identical copy of it. Public ledger have any changes or update is made it will reflected and copied to all participants. Underlying distributed ledgers is the same technology that is used by blockchain which is the technology that is used to cryptocurrencies. Distributed computing in blockchain is working under decentralized public ledger; distributed computing blockchain technology consists of two different methodologies: public blockchain and private blockchain. This chapter explains the importance of distributed computing in blockchain, platforms, barriers, and privacy challenges of distributed computing.

Keywords Public ledger · Distributed computing · Decentralization · Nodes

V. Ramalingam (✉) · C. Ramesh Kumar
Galgotias University, Greater Noida, UP, India
e-mail: r.vijay@galgotiasuniversity.edu.in; c.ramesh@galgotiasuniversity.edu.in

D. Mariappan
Galgotia College of Engineering and Technology, Greater Noida, UP, India
e-mail: dinesh.babu@galgotiacollege.edu

S. Premkumar
Annamalai University, Chidambaram, Tamil Nadu, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_4

1 Introduction

1.1 Public Ledger

An open record gets its name from the deep-rooted record-keeping framework that was utilized to record data like farming item costs, news, and investigation. It was accessible for overall population seeing just as for confirmation.

As digital currency-based blockchain frameworks rose, which likewise depended on a comparable record-keeping and open check component, the utilization of open record term picked up prevalence in the realm of cryptographic money. This article investigates digital currency open records, their working, and the difficulties they face.

1.1.1 Public Ledgers: Where Everything Gets Stored

Cryptographic money is a scrambled, decentralized advanced cash that encourages the trading of significant worth by the exchange of crypto tokens between arranging members. The open record is utilized as a record-keeping framework that keeps up members' personalities unreliable and (pseudo-)unknown structure, their particular cryptographic money adjusts, and a record book of all the real exchanges executed between organizing members.

To draw an equal, consider composing a check to a companion or making an online exchange to his ledger, state for $100.

In the two cases, the subtleties of the exchange will be refreshed in the bank's records – the sender's record is charged with $100, while the recipient's record is credited by a similar sum. The bank's bookkeeping frameworks keep the record of parities and furthermore guarantees that the sender's record has adequate assets, in any case, the check ricochets or the online exchange isn't permitted. If the sender has just $100 in his record and he gives two $100 checks, the request where the checks are introduced figures out who gets the cash and whose check skips.

The exchange's subtleties in the bank's records can be questioned and checked by the two gatherings between whom the exchange occurred. Furthermore, the bank record is available just by the assigned bank authorities and the concerned (focal) specialists like the assessment division of the administration on a need premise. Nobody else can approach those subtleties.

1.1.2 Public Ledgers Work the Same Way as Bank Records, Though with a Few Differences

Like the bank records, the exchange subtleties on a digital currency open record can be confirmed and questioned by the two executing members. Be that as it may, no focal position and other system members can know the personality of the members.

Exchanges are permitted and recorded simply after reasonable confirmation of the sender's liquidity, else, they are disposed of.

Since no focal power controls or keeps up the record records, how is reasonableness managed on cryptographic money records?

1.1.3 How Does Public Ledger Work?

Genuinely, an open record can be seen as an information the board or capacity framework, like a database arrangement of bank records. A blockchain is a type of an open record, which is an arrangement (or chain) of squares on which exchange subtleties are recorded after appropriate validation and confirmation by the assigned system members. The account and capacity of every affirmed exchange on such open records start directly from the creation and beginning of a digital currency's working. As a square is loaded up with exchange subtleties, new ones are mined and are added to the blockchain by the system members called diggers.

Select system members, frequently called full hubs, keep up a duplicate of the entire record on their gadgets that are associated with the digital currency arrange. Contingent upon the members' advantage and their spread over the globe, the open record gets circulated, as the interface and add to the blockchain organize exercise to keep it light-footed and useful.

Since hundreds and thousands of such members keep up a duplicate of the record, everybody knows the genuine condition of the system as far as who holds what number of crypto token, what exchanges are legitimate to be recorded, and forestall any abuse like twofold spending. A mix of the different inherent highlights of the open record, similar to agreement calculation, encryption, and prize component, guarantees that the members' characters are secured, and just certifiable exchanges are carried on the system.

1.1.4 Blocks in Blockchain

Blocks are documents where information on the Bitcoin arrange is forever recorded. A square records a few or the entirety of the latest Bitcoin exchanges that have not yet entered any earlier squares. Along these lines, a block resembles a page of a record or record book. Each time a block is "finished," it offers a path to the following block in the blockchain. A block is in this manner a perpetual store of records which, when composed, can't be adjusted or evacuated.

Block hold clumps of legitimate exchanges that are hashed and encoded into a Merkle tree. Each block remembers the cryptographic hash of the earlier block for the blockchain, connecting the two. The connected squares structure a chain. This iterative procedure affirms the honesty of the past square, right back to the first beginning square.

In some cases, separate squares can be delivered simultaneously, making a transitory fork. Notwithstanding a protected hash-based history, any blockchain has a

predetermined calculation for scoring various variants of history so one with a higher score can be chosen over others. Block not chosen for incorporation in the chain are called vagrant blocks. Peers supporting the database have various renditions of the history every once in a while. They keep just the most noteworthy scoring variant of the database known to them. At whatever point a companion gets a higher-scoring rendition (generally the old form with a solitary new square included), they expand or overwrite their database and retransmit the improvement to their friends. There will never be an assurance that a specific section will stay in the best form of history until the end of time. Blockchains are regularly worked to include the score of new squares onto old squares and are offered motivations to stretch out with new squares as opposed to overwriting old squares. Along these lines, the likelihood of a passage turning out to be supplanted diminishes exponentially as more squares are based on the head of it, in the end getting low.

1.1.5 Block Time

The block time is the normal time it takes for the system to create one additional block in the blockchain. Some blockchains make another square as much of the time as at regular intervals. When of block consummation, the included information gets evident. In digital money, this is basically when the exchange happens, so a shorter block time implies quicker exchanges. The square which is an ideal opportunity for Ethereum is set to somewhere in the range of 14 and 15 seconds, while for Bitcoin it is on normal 10 minutes.

2 Overview of Distributed Computing

2.1 Bitcoin Shared Network

Bitcoin uses imparted development to work to no central position or banks; supervising trades and the giving of Bitcoins are done in general by the framework. Bitcoin is open-source; its structure is open, nobody has or controls Bitcoin, and everyone can take part. Through a significant part of its noteworthy properties, Bitcoin licenses empowering utilizes that couldn't be made sure about by any past portion structure.

The Bitcoin mastermind is shared portions compose that chips away at a cryptographic show. Customers send and get Bitcoins, the units of cash, by conveying painstakingly checked messages to the framework using Bitcoin advanced cash wallet programming. Trades are recorded into an appropriated, replicated open database known as the blockchain, with understanding achieved by a proof-of-work structure called mining.

The framework requires an immaterial structure to share trades. An extraordinarily selected decentralized arrangement of volunteers is satisfactory. Messages are imparted on the best effort reason, and center points can leave and rejoin the framework uninhibitedly. Upon reconnection, a center point downloads and checks new squares from various center points to complete its close-by copy of the blockchain.

Mutual (P2P) preparing or frameworks organization is a passed-on application designing that bundles endeavors or remaining weights between peers. Companions are comparably exceptional, equipotent individuals in the application. They are said to shape a mutual arrangement of centers. Mates make a fragment of their benefits, for instance, taking care of intensity, plate accumulating, or framework transmission limit and directly available to other framework individuals, without the necessity for central coordination by workers or stable hosts. Companions are the two suppliers and purchasers of advantages, as opposed to the standard client-worker model in which the use and adaptability of benefits are isolated. Rising helpful P2P systems are going past the time of colleagues doing relative things while sharing resources and are scanning for varying companions that can secure outstanding resources and abilities to a virtual system, thus empowering it to take an interest in progressively significant tasks past those that can be developed by particular companions, yet that is favorable to all the friends (Fig. 1).

While P2P frameworks had recently been utilized in numerous application areas, the engineering was promoted by the record-sharing framework Napster, initially discharged in 1999. The idea has enlivened new structures and ways of thinking in numerous regions of human collaboration. In such social settings, distributed as an image alludes to the populist long-range interpersonal communication that has risen all through society, empowered by Internet advancements all in all.

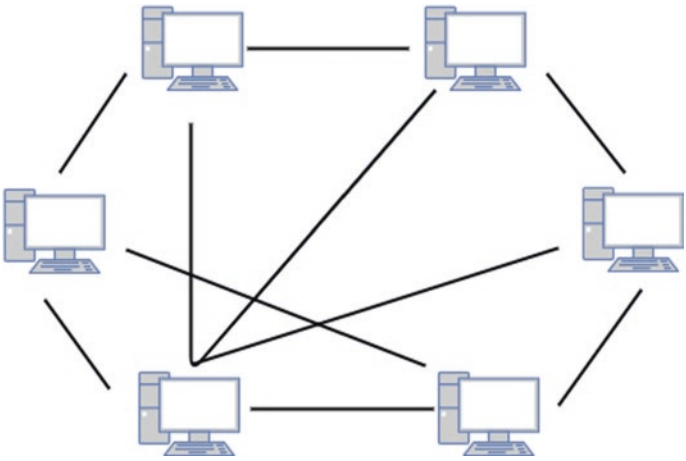


Fig. 1 Peer-to-peer connection

Fig. 2 Transaction

2.2 *Transaction in Bitcoin Network*

As another client, you can begin with Bitcoin without understanding the specialized subtleties. When you've introduced a Bitcoin wallet on your PC or cell phone, it will produce your first Bitcoin address, and you can make more at whatever point you need one. You can reveal your addresses to your companions with the goal that they can pay you or the other way around. This is really like how email functions, but then again, actually Bitcoin addresses ought to be utilized just a single time (Fig. 2).

The blockchain is a mutual *open record* on which the whole Bitcoin organize depends. Every single affirmed exchange is remembered for the blockchain. It permits Bitcoin wallets to compute their spendable equalization with the goal that new exchanges can be checked in this way guaranteeing they're possessed by the high roller. The trustworthiness and the sequential request of the blockchain are authorized with cryptography (Fig. 3).

2.3 *Exchanges: Private Keys*

A trade is a trade of noteworthy worth between Bitcoin wallets that gets associated with the blockchain. Bitcoin wallets let sleeping dogs lie a touch of data called a private key or seed, which is used to sign trades, giving a numerical affirmation that they have begun from the owner of the wallet. The imprint also shields the trade from being balanced by anybody once it has been given. All trades are imparted to the framework and for the most part begin to be avowed inside 10–20 minutes, through a method called mining (Fig. 4).

2.4 *Handling: Mining*

Mining is a coursed understanding structure that is used to avow pending trades by recollecting them for the blockchain. It maintains a consecutive solicitation in the blockchain, makes sure about the unbiasedness of the framework, and licenses different PCs to surrender to the state of the system. To be asserted, trades must be full in a square that fits extreme cryptographic norms that will be affirmed by the framework. These rules keep past squares from being balanced considering the way that

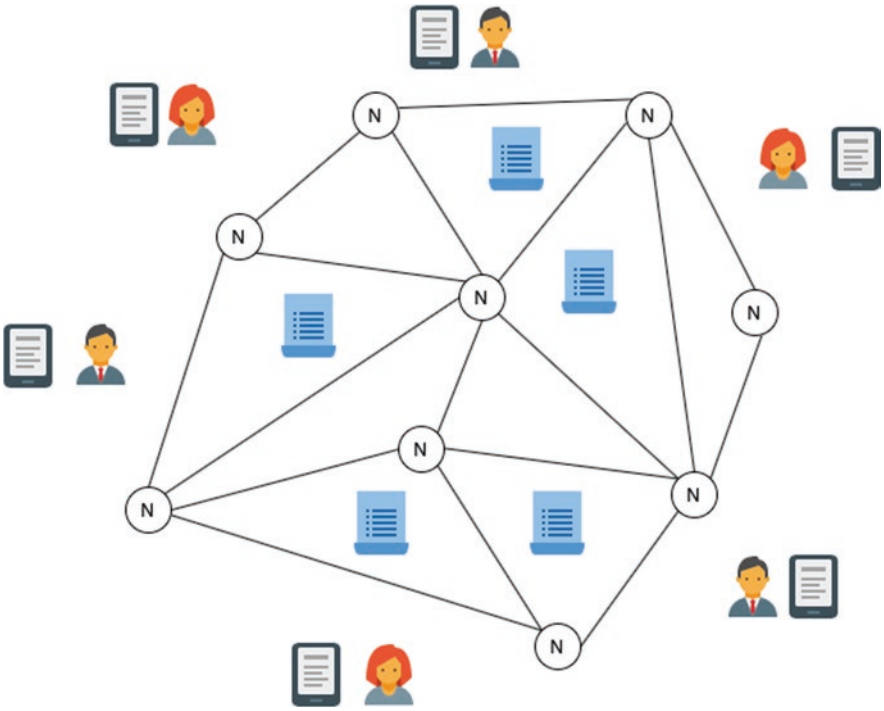


Fig. 3 Shared public ledger

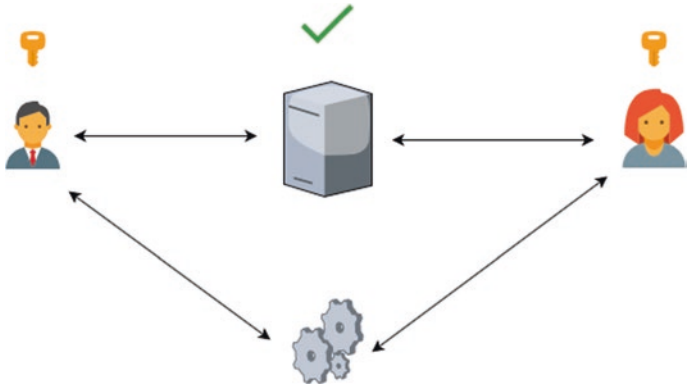


Fig. 4 Key exchange

doing so would discredit all the resulting squares. Mining also makes what could be contrasted with a genuine lottery that keeps any individual from successfully adding new squares progressively to the blockchain. Thus, no social event or individuals can control what is associated with the blockchain or override bits of the square chain to move back their spending (Fig. 5).

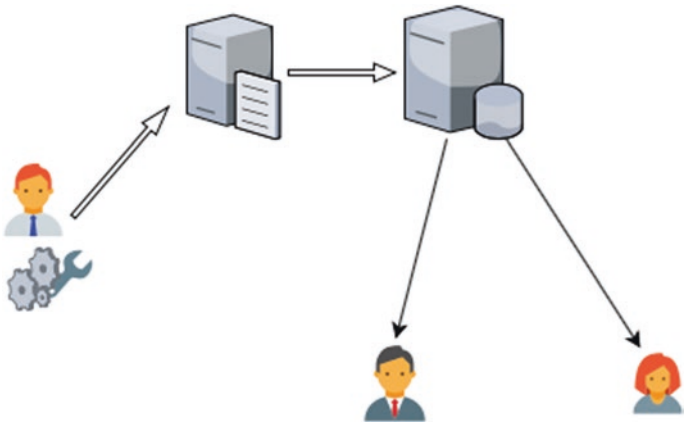


Fig. 5 Block mining

2.5 Bitcoin Mining

Mining is the route toward adding trade records to Bitcoin's open record of past trades (and a "mining rig" is a conversational moral story for a single PC structure that plays out the crucial computations for "mining"). This record of past trades is referred to as the blockchain as it is a chain of squares. The blockchain serves to assert trades to the rest of the framework as having happened. Bitcoin centers use the blockchain to perceive certified Bitcoin trades from attempts to re-spend coins that have recently been spent elsewhere.

Mining is purposely expected to be resource genuine and irksome with the objective that the quantity of squares found each day by excavators remains predictable. Particular squares must contain confirmation of work to be seen as real. This affirmation of work is checked by other Bitcoin center points each time they get a square. Bitcoin uses the hash cash check of work.

The principle job of mining is to set the verifiable scenery of trades in a way that is computationally outlandish to change by any one substance. By downloading and checking the blockchain, Bitcoin center points can show up at an understanding about the mentioning of events in Bitcoin.

Mining is also the segment used to bring Bitcoins into the structure: miners are paid any trade charges similarly as an "apportionment" of as of late made coins. These two viably scatter new coins in a decentralized manner similarly as convincing people to offer security to the structure.

Bitcoin mining is affirmed since it takes after the mining of various items: it requires exertion, and it bit by bit makes new units open to any individual who wishes to share. A huge qualification is that it smoothly doesn't depend upon the proportion of mining. All-around changing outright digger hash power doesn't change what number of Bitcoins are made as time goes on.

2.6 Difficulty

2.6.1 The Computationally Difficult Problem

Mining a square is troublesome because the SHA-256 hash of a square's header must be lower than or equivalent to the objective for the square to be acknowledged by the system. This issue can be streamlined for clarification purposes: the hash of a square should begin with a specific number of zeros. The likelihood of ascertaining a hash that begins with a large number is low; along these lines, numerous endeavors must be made. To create another hash in each cycle, a nonce is augmented. See Proof of Work for more data.

2.6.2 The Difficulty Metric

The trouble is the proportion of the fact that it is so hard to locate another square contrasted with the most effortless it can ever be. The rate is recalculated every 2016 squares to worth with the end goal that the past 2016 squares would have been created in precisely one fortnight (14 days) had everybody been mining at this trouble. By and large, one square at regular intervals.

As more excavators join, the pace of square creation increments. As the pace of square age expands, the trouble ascends to redress, which has an adjusting of impact because of diminishing the pace of square creation. Any squares discharged by malignant excavators that don't meet the necessary trouble target will basically be dismissed by different members in the system.

2.7 Reward

At the point when a square is found, the pioneer may grant themselves a specific number of Bitcoins, which is settled upon by everybody in the system. As of now, this abundance is 12.5 Bitcoins; this worth will split every 210,000 squares. See Controlled Currency Supply.

Furthermore, the digger is granted the charges paid by clients sending exchanges. The charge is a motivator for the digger to remember the exchange for their square. Later on, as the quantity of new Bitcoin diggers which are permitted to make in each square diminishes, the expenses will make up a substantially more significant level of mining pay.

2.8 The Mining Environment Hardware

2.8.1 FPGA Module

Clients have utilized different sorts of equipment after some time in my squares. Equipment particulars and execution insights are nitty-gritty on the Mining Hardware Comparison page.

2.8.2 CPU Mining

Early Bitcoin customer renditions permitted clients to utilize their CPUs to mine. The approach of GPU mining made CPU mining monetarily incautious as the hash pace of the system developed to such an extent that the number of Bitcoins delivered by CPU mining became lower than the expense of capacity to work a CPU. The choice was subsequently expelled from the center Bitcoin customer's UI.

2.8.3 GPU Mining

GPU mining is definitely quicker and more effective than CPU mining. See the principle article: Why a GPU mines quicker than a CPU. An assortment of well-known mining rigs has been archived.

2.8.4 FPGA Mining

FPGA mining is an extremely effective and quick route to mine, tantamount to GPU mining and radically beating CPU mining. FPGAs regularly devour extremely modest quantities of intensity with generally high hash appraisals, making them more suitable and effective than GPU mining. See Mining Hardware Comparison for FPGA equipment determinations and measurements.

2.8.5 ASIC Mining

An application-explicit incorporated circuit, or ASIC, is a microchip planned and produced for a quite certain reason. ASICs intended for Bitcoin mining were first discharged in 2013. For the measurement of intensity they devour, they are tremendously quicker than every single past innovation and as of now have made GPU mining monetarily.

2.8.6 Mining Administrations (Cloud Mining)

Mining contractual workers give mining administrations execution determined by contract, frequently alluded to as a "mining contract." They may, for instance, lease a particular degree of digging limit with regard to a set cost at a particular length.

3 Importance of Disseminated Registering in the Blockchain

3.1 Transaction

An exchange is an exchange of Bitcoin esteem that is communicated to the system and gathered into squares. An exchange regularly references past exchange yields as new exchange inputs and devotes all information Bitcoin qualities to new yields. Exchanges are not encoded, so it is conceivable to peruse and see each exchange at any point gathered into a square. When exchanges are covered under enough affirmations, they can be viewed as irreversible. Standard exchange yields choose addresses, and the reclamation of any future data sources requires an applicable mark.

All exchanges are noticeable in the blockchain and can be seen with a hex proofreader. A blockchain program is where each exchange included inside the blockchain can be seen in intelligible terms. This is valuable for seeing the specialized subtleties of exchanges in real life and for confirming installments.

3.2 First Things First

Arithmetic alone structures the premise of digital money, a type of virtual cash. Cryptography is by definition "the specialty of illuminating or composing codes." But as far as arithmetic and PC coding is concerned, cryptography utilizes calculations and conventions to make sure about scramble data into an encoded design. Envision cautiously setting letters into boggle, illuminating a few words. Encryption is only the activity of stirring up that boggle board, while decoding is the way toward putting the first messages back together. Generally, it's a scrambled string of information that has been encoded to imply a solitary, explicit unit of money. Tackling numerical issues in light of on cryptography – or the specialty of composing codes – produces digital money.

3.3 Tokens

Tokens are fundamental to get a genuine hold on digital forms of money. They're the number of computerized assets you control on a given stage. As referenced previously, an advanced wallet stores them and got to with a key, which can be reassigned to another person. Two sorts of tokens exist.

In the first place, it is a local token. This kind of token has an inborn utility. It shapes the centerpiece of a blockchain. In other words, a blockchain couldn't run without a local token. Frequently, they're utilized as a motivator to approve exchanges or make squares.

A conveyed accord guarantees an agreement of information among hubs in a circulated framework or agrees on a proposition. This subject might be exceptionally recognizable to any professionals that work with appropriated frameworks, for example, HDFS, MQ, ZooKeeper, Kafka, Redis, and Elasticsearch. With the fast turn of events and the expanding multifaceted nature of dispersed systems, designers have consistently been investigating potential answers for taking care of this tireless issue in both hypothesis and practice.

Next, with the ascent of blockchain innovation, particularly open blockchains in open systems and private blockchains in permissioned systems, this accord issue has indeed gotten a lot of consideration and should be considered from another viewpoint.

3.4 Issues and Challenges of Distributed Consensus

To completely comprehend disseminated agreement, we have to initially fabricate a comprehension of the highlights of a circulated organize. What are the primary highlights and qualities of a disseminated organization? Or on the other hand, what are some potential issues associated with a conveyed arrangement? We should investigate a portion of these inquiries in this segment of this article.

3.5 Crash Fault

To start with, how about we consider money issues. An accident deficiency in a conveyed arrange regularly might be identified with one of the accompanying issues:

- Nodes or reproductions may encounter personal time whenever, quit running for a brief timeframe, and recuperate later.
- The system might be hindered whenever.
- A sent message might be lost during conveyance and can't be gotten.

- A sent message might be postponed and gotten after quite a while.
- Messages may encounter the faulty issue during the conveyance procedure.
- The system might be separated. For instance, because of helpless correspondence between bunches in China and the USA, the whole system might be separated into two subsystems for the China groups and US groups, for example.

3.6 The Byzantine Fault

The accident flaws depend on a straightforward suspicion: either hub don't work or react regularly, or despite the fact that they work and react typically, they can't execute irregularity; in other words, being inert is all right for them,

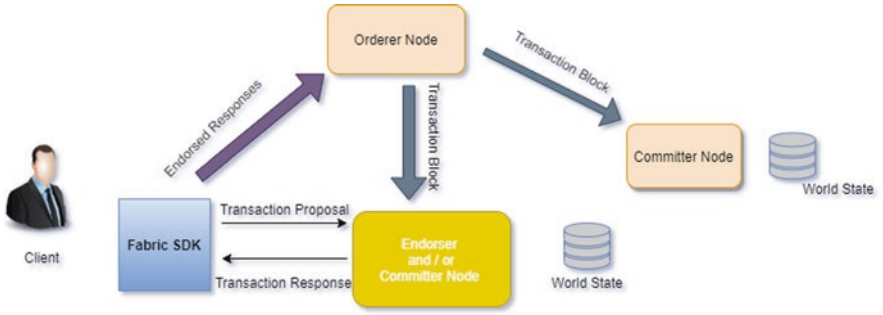
Byzantine began from Lamport's paper. It is no embellishment to state that Byzantine's adaptation to internal failure (BFT) is the most intricate and thorough resilience model. By relationship, a few officers plan an assault on a stronghold together, and each broad can decide to begin the assault or retreat. In any case, to effectively take the mansion, all the commanders must act simultaneously. Next, given that the officers are excessively far from one another to utilize direct correspondence, delegates are accustomed to conveying messages. Be that as it may, messages are not solid. They may effectively convey messages after an exceptionally prolonged stretch of time, neglect to convey messages, or even change with messages. The officers may not be solid; either, for instance, one of them might be a deceiver who doesn't act under the arrangement. The delivery people in this story speak to correspondence diverts in circulated systems, and the officers speak to hubs.

4 Platforms to Develop Blockchain

4.1 Hyperledger Fabric Components and Architecture

Hyperledger Fabric is a permissioned blockchain structure, with measured engineering (attachment and play). It uses holder innovation to have brilliant agreements (Chaincode) which contains the application rationale.

Before heading off to every part in detail, let us see a significant level of exchange stream and fundamental segments included.



- Membership Service Provider (MSP)
- Client
- Peer
- Orderer

4.1.1 Participation Service Provider (MSP)

The participation specialist co-op (MSP) is a segment that characterizes the standards wherein personalities are approved, validated, and permitted access to a system. The MSP oversees client IDs and verifies customers who need to join the system. This incorporates giving qualifications to these customers to propose exchanges. The MSP utilizes a certificate authority, which is a pluggable interface that checks and disavows client authentications upon affirmed personality. The default interface utilized for the MSP is the Fabric-CA API. Be that as it may, associations can actualize an external certificate authority of their decision. Therefore, a solitary Hyperledger Fabric system can be constrained by numerous MSPs, where every association brings its top choice.

There are two kinds of MSPs:

1. *Local MSP*: It characterizes users (clients) and nodes (peers, orderers). It characterizes who has regulatory or participatory rights at that level.
2. *Channel MSP*: It characterizes regulatory and participatory rights at the channel level.

4.1.2 Customer

Customers are applications that follow up for the benefit of an individual to propose exchanges on the system. The customer utilizes a Fabric SDK to speak with the system. The customer speaks with the SDK to read or write the information in a Fabric blockchain and an in-state DB. Indeed, even the customer is given an

endorsement from the CA position to ensure that a substantial customer has started the exchange over the system.

4.1.3 MSP/Hub

A "hub" is just an intelligent capacity as numerous hubs of various kinds can run on the equivalent physical server. What tallies are how hubs are assembled in "trust areas" and related to legitimate elements that control them.

There are three sorts of MSP:

1. *Client*: A customer that presents a real exchange summons to the endorsers and communicates the exchange proposition to requesting administration. So, customers speak with the two companions and the requesting administration.
2. *Peer*: A hub that submits exchanges and keeps up the state and a duplicate of the record. A companion gets requested state refreshes as squares from the requesting administration and keeps up the state and the record. Additionally, friends can have an uncommon endorser job. The unique capacity of a supporting friend happens concerning a specific chain code and comprises of underwriting an exchange before it is submitted.
3. *Ordering administration hub or orderer*: a hub running the correspondence administration that executes a conveyance ensure, for example, nuclear or all-out request communication.

4.1.4 Types of Peers

- *Endorsing Peer*: Endorsing peers is an extraordinary kind of submitting peers who have an extra job to underwrite an exchange. They underwrite the exchange demand which originates from the customer. Each underwriting peer has a duplicate of a brilliant agreement introduced and a record. The fundamental capacity of an endorser is to recreate the exchange. It is executed dependent on the shrewd agreement on the individual duplicate of the record and creates the read/write sets which are sent to client. Despite the fact that during reproduction, the exchange isn't focused on the record.
- *Committing Peer*: Peers who submit the square which is gotten from the ordering administration, in their duplicate of the blockchain. This square contains the rundown of exchanges where submitting companions approve every exchange and imprint it as either substantial or invalid and focus on the square. All exchanges either legitimate or invalid are completely dedicated to blockchain for future review purposes.
- *Anchor Peer*: As a Fabric system can reach out over various associations, we need a few friends to have correspondence over an association. Not all companions can do this; however, these are uncommon friends who are just approved to

do so which are only anchor peer. The grapple peers are characterized in channel setup.

- *Leading Peer*: Leader peers are the individuals who impart or scatter messages from ordering administration to different friends in a similar association. These companions utilize the gossip convention to ensure that each friend gets the message. Driving friends can't convey over an association. In the event that any leading companion isn't reacting or is out of the system, at that point we can choose the main friend from accessible companion dependent on casting a ballot or arbitrarily pick one.

4.1.5 Orderer

In a blockchain organization, exchanges must be kept in touch with the mutual record in a predictable request. The request for exchanges must be set up to guarantee that the updates to the world state are substantial when they are focused on the system, not at all like the Bitcoin blockchain, where requesting happens through the unraveling of a cryptographic riddle or mining. Hyperledger Fabric permits the associations running the system to pick the requesting instrument that best suits that arrangement. These measured quality and adaptability make Hyperledger Fabric amazingly beneficial for big business applications.

4.2 Overview of Ripple and Corda

4.2.1 Ripple (XRP)

XRP is like Bitcoin, yet it amplifies quicker than Bitcoin can scale to give comparable number exchanges every second to Visa. Every exchange keeps going around 4 seconds and is deterministic. Furthermore, every exchange in XRP is approved by validators, and everyone can turn into a validator. It's additionally spared in the blockchain record. XRP has its agreement system. Wave has a decentralized trade and discretionary resources. Wave has been condemned for not being genuinely decentralized or for utilizing just a couple of center approval hubs.

4.2.2 Corda

R3 Corda is a semi-private permissioned blockchain that essentially targets explaining budgetary cases. Each system has a porter help that has a lot of KYC decides that must be given to join the system. If a friend is acknowledged, a declaration is conceded that will help distinguish proof inside the system. Of course, data about exchanges is just mutual with the individuals who take part in the exchange.

There is no single focal store of information. Rather, every hub keeps up a different database. Subsequently, each companion just observes a subset of realities on the record, and no friend knows about the real factors in a record. In Corda, exchanges to be acknowledged must accomplish two sorts of accord: legitimacy and uniqueness. The supposed notaries deal with it – they can be either unified hubs or circulated utilizing a pluggable agreement calculation like RAFT or BFT or some other. Keen agreements in Corda actualize any JVM language, be that as it may Kotlin and Java which are most advanced. The agreements can connect a Legal writing archive that can be depended upon on account of legitimate questions in reality.

Smart contracts in Corda consist of three elements:

State objects – stores the information that is checked by the agreement. Speak to the condition of a record. Exist in yield and information.

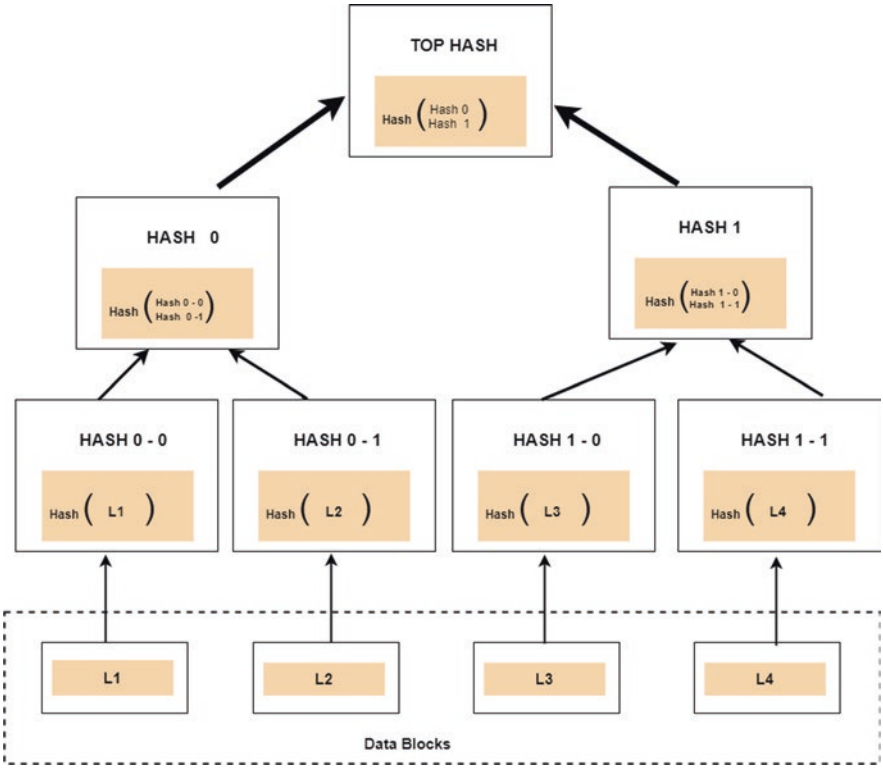
Comments – extra information for the exchange they are parametrizing the agreement. Gone as a contribution to contract.

Confirmation function – approval work as it approves the exchange. On the off chance that the exchange is returned, at that point it's effective if a special case happens we have disappointment Contracts just approve the exchanges in an unadulterated and stateless manner, they check capacities they don't interface with the outside world. An exchange contains all info and yield states. Agreements are bundled to CorDapp (Corda-disseminated application) with different articles. Different items that CorDapp comprise of are services (Oracles and Notaries) and flows. Streams are contained in the purported FlowLogic class and are utilized for taking care of business stream situations.

Prophet administrations give the information from the outside world to the record. The as-of-now referenced Notaries run accord calculation and keep a similar exchange from being run twice. Public accountants can likewise approve an exchange on the off chance that they wish to. CorDapps are bundled to a container and sent on a hub premise.

4.3 Merkle Tree

Merkle tree is a twofold inquiry tree, worked with hash pointers; we can do logarithmic time enrollment proofs and non-participation proofs on the off chance that we sort the tree and it is effective. All the more for the most part, for reasons unknown, we can utilize hash pointers in any pointer-based information structure as long as the information structure doesn't have cycles.



4.3.1 Merkle Trees in Bitcoin

The cryptographic hash work utilized by Bitcoin is the SHA-256 calculation. This means "Secure Hashing Algorithm," whose yield is a fixed 256 bits long. The fundamental capacity of Merkle trees in Bitcoin is to store and in the long run prune exchanges in each square.

As referenced before, hinders in a blockchain are associated through hashes of the past square. In Bitcoin, each square contains the entirety of the exchanges inside that hinder just as the square header which comprises of:

- Block version number
- Previous block hash
- Timestamp
- Mining difficulty target
- Nonce
- Merkle root hash

5 Barriers to Implementing Blockchain

5.1 Creation of Coin

5.1.1 Where Cryptocurrency Comes From

Digital money is made by code. By and large, new coins are made when exchanges are affirmed by a procedure known as mining.

All things considered, while coins like Bitcoin and Ethereum use mining, only one out of every odd cryptographic money utilizes mining to produce new coins, and coins can be made in some different manners too.

How precisely coins are made relies upon what is characterized by a given cryptographic money's code. For instance, the digital currency may make a few tokens upon dispatch as designer rewards or cryptographic money may payout tokens as profits each month.

More Points to Consider to Understand How Cryptocurrency is Created:

- *Cryptocurrency is programming*. Each capacity from how exchanges are recorded, to how information is put away, is directed by code.
- Especially for digital forms of money whose principle work is to go about as cash, cryptographic money exchanges are normally put away in a sort of database known as a blockchain (different cryptos utilize one of a kind innovation, yet the significance is the equivalent).
- What we consider as cryptographic money, for instance, 1 Bitcoin, is simply numbers recorded on a digital currency's blockchain. Another word for that substitute for esteem is "token" (regularly additionally called a "coin").
- Cryptocurrencies are made by calculations that depend on cryptography. That is the reason it is known as the "crypto" money. Each exchange identifies with extraordinary cryptographic codes that protected the system.
- Cryptocurrency programming is decentralized and disseminated, which means it is facilitated on numerous people groups' PCs over the world rather than just on one worker by one organization.
- The calculations for the most part are composed to grant coins to PCs who add exchanges to the blockchain. The way toward adding exchanges to the blockchain is known as mining.
- The code of the digital currency characterizes things like greatest flexibly, mining rewards, and so on.
- Thus, for most cryptographic forms of money, the fundamental way new coins are made is by individuals everywhere throughout the world running equipment that adds exchanges to the blockchain. Something else, digital money tokens are made by different systems contained in a cryptographic money's product.
- Lastly, the code for practically all cryptographic forms of money is open, so anybody can check how coins are made.

Reality: Because the gracefully and swelling of given cryptographic money are characterized by code, it is known forthright whether a coin is inflationary or deflationary. The best way to change that is to change the product. To change the product, most of the PCs running the product need to concede to an overhaul. By and large, something like a change to the pace of gracefully would bring about a "fork" (another adaptation of the product). Given the entirety of this, it is impossible the gracefully or pace of issuance of a coin like Bitcoin could ever be changed. In this manner, we can be certain the main coins that will be given are the ones characterized by the code.

5.2 Payments and Double-Spending

At the point when utilized accurately, Bitcoin's base layer exchanges on the blockchain are irreversible and last. It's no distortion to state that the aggregate of Bitcoin's arrangement of blockchain, mining, verification of work, trouble, and so on exist to deliver this history of exchanges that is computationally illogical to alter.

In the writing on electronic money, this property frequently alluded to as "taking care of the twofold spending issue." Twofold spending is the aftereffect of effectively going through some cash more than once. Bitcoin clients shield themselves from twofold spending extortion by hanging tight for affirmations while accepting installments on the blockchain; the exchanges become increasingly irreversible as the number of affirmations rises.

Other electronic frameworks forestall twofold spending by having an ace definitive source that keeps business rules for approving every exchange. Bitcoin utilizes a decentralized framework, where an agreement among hubs following a similar convention and verification of work is filled in for a focal position. This implies Bitcoin has unique properties not shared by brought together frameworks. For instance, on the off chance that you keep the hidden key of a Bitcoin mystery and the exchange has enough affirmations, at that point, no one can take the Bitcoin from you regardless of what reason or how great the reason. Ownership of Bitcoin isn't upheld by business rules and strategy, yet cryptography and game hypothesis.

Since Bitcoin exchanges can be conclusive, shippers don't have to issue clients for additional data like charging address, name, and so on, so Bitcoin can be utilized without enlisting a genuine name or barring clients dependent on age, nationality, or residency. Certainty in exchanges implies savvy agreements can be made with a "code-is-law" ethos.

5.3 Types of Spending Attack

5.3.1 Race Assault

Dealers and traders who acknowledge a payment promptly on observing "0/unverified" are presented to the exchange being switched. An endeavor at extortion could work that the fraudster sends an exchange paying the vendor legitimately to the shipper and sends a clashing exchange spending the coin to himself to the remainder of the system. The second clashing exchange will probably be mined into a square and acknowledged by Bitcoin hubs as certifiable.

Vendors can play it safe (e.g., impair approaching associations, just interface with very much associated hubs) to reduce the danger of a race assault; however, the hazard can't be dispensed with. Consequently, the cost/advantage of the hazard should be viewed as, while tolerating payment on 0/unverified when there is no plan of action against the aggressor.

5.3.2 Finney Assault

Another assault the dealer or shipper is presented to while tolerating payment on 0/unverified. The Finney assault is a fake twofold spend that requires the interest of a digger once a square has been mined [2]. The danger of a Finney assault can't be dispensed with paying little heed to the insurances taken by the shipper, yet some excavator hash power is required and a particular arrangement of occasions must happen. Much the same as with the race assault, a broker or shipper ought to think about the cost/advantage while tolerating installment on only one affirmation when there is no plan of action against the aggressor.

5.3.3 Vector76 Assault

Additionally alluded to as a one-affirmation assault, it is a mix of the race assault and the Finney assault to such an extent that an exchange that even has one affirmation can in any case be turned around. The equivalent defensive activity for the race assault (no approaching associations, express friendly association with a very much associated hub) altogether lessens the danger of this happening.

It is significant that an effective assault costs the assailant one square – they have to "penance" a square by not communicating it and as opposed to handing off it just to the assaulted hub.

5.3.4 Blockchain Reorganization Assault

Additionally called an elective history assault, this assault gets an opportunity to work regardless of whether the trader hangs tight for certain affirmations yet requires generally high hash rate and danger of huge cost in squandered power to the assaulting excavator.

The assailant submits to the dealer/organize an exchange which pays the shipper while secretly mining an option blockchain fork in which a fake twofold spending exchange is incorporated. Subsequent to sitting tight for n affirmations, the vendor sends the item. On the off chance that the aggressor happened to discover more than n hinders now, he discharges his fork and recaptures his coins; else, he can attempt to keep expanding his fork with the desire for having the option to find the system. In the event that he never figures out how to do this, at that point the assault comes up short, the assailant has squandered a lot of power and the installment to the shipper won't be turned around.

5.3.5 Majority Assault

It is likewise alluded to as a 51% assault or >50% assault. On the off chance that the assailant controls the greater part of the system hash rate, the beforehand referenced alternative history assault has a likelihood of 100% to succeed. Since the assailant can create squares quicker than the remainder of the system, he can basically endure with his private fork until it turns out to be longer than the branch worked by the genuine system, from whatever impediment.

No measure of affirmations can forestall this assault; in any case, hanging tight for affirmations builds the total asset cost of playing out the assault, which might make it unrewarding or postpone it long enough for the conditions to change or more slow-acting synchronization strategies to kick in. Bitcoin's security model depends on no single alliance of excavators controlling the greater part of the mining power. An excavator with over half hash power is boosted to diminish their mining power and reframe from assaulting for their mining gear and Bitcoin salary to hold its worth.

6 Privacy Challenges

6.1 Introduction

Blockchain is a disseminated document framework where members keep duplicates of the record and concede to changes by the accord. This document is made out of squares, where each square incorporates a cryptographic mark of the past square,

making a changeless record. Frameworks based on blockchain are viewed as more secure than the current ones based on the web foundation dependent on TCP/IP.

In any case, blockchain has innovation moves identified with versatility, inertness, execution, and security. Additionally, the blockchain has numerous operational issues. For instance, logging and observing which are fundamental for big business situations have not been tended to yet.

Other than that, applications based on blockchain still can have security issues, regardless of whether blockchain is water/air proof. On the off chance that one needs open availability, designers can place that in your application. Without a decent structure of highlights, applications can in any case be powerless and exploitable. For databases, programmers can reproduce the document to get their hands on classified agreement data.

6.2 To the Community

Blockchain can be thought of as a deliberation of the essential component of advanced money like Bitcoin. This dispersed reflection can have numerous applications and be an answer for web security, protection, and straightforwardness in numerous particular situations. Along these lines, the web network has to think about the uses of blockchain and its effect on security. Dissimilar to Bitcoin as a sort of money, blockchain is for the decentralization of business sectors all the more for the most part and examines the exchange of numerous different sorts of advantages past cash, from the formation of a unit of significant worth through each time it is moved or partitioned.

The key though is that the decentralized exchange record usefulness of the blockchain could be utilized to enroll, affirm, and move all way of agreements and property. Every single money-related exchange could be rehashed on the blockchain, including stock, private value, crowdfunding instruments, securities, common assets, annuities, benefits, and all ways of subsidiaries.

Open records, as well, can be moved to the blockchain: land and property titles, vehicle enlistments, permit to operate, marriage testaments, and passing declarations. Advanced personality can be affirmed with the blockchain through safely encoded driver's licenses, character cards, visas, and voter enlistments. Private records, for example, IOUs, advances, contracts, wagers, marks, wills, trusts, and escrows, can be put away.

6.3 Applications in Identity Authentication

The requirement for blockchain-based character confirmation is especially remarkable in the web age. While there exist to some degree defective frameworks for building up close to home personality in the physical world, as social security

numbers, drivers' licenses, and even travel papers or national character cards, there is no identical framework for making sure about either online validation of our personalities or the personality of computerized substances. Facebook accounts, presently regularly utilized as the login for various advanced applications, and media get to control (MAC) addresses and may approach, yet both can scarcely work as dependable types of distinguishing proof when they can be changed freely.

6.4 Online Identity

A few blockchain new businesses are hoping to utilize blockchain for online personality. A ShoCard, for instance, is an advanced personality that secures customer protection. ShoCard endeavors to be as straightforward and use as indicating a driver's permit and at the same time be secure to the point that a bank can depend on it. The key is that the ShoCard Identity Platform is based on an open blockchain information layer, so as an organization isn't putting away information or keys that could be undermined. As indicated by ShoCard, all character information is scrambled, hashed, and put away in the blockchain, where it can't be messed with or adjusted. A beginning up in a comparable vein that overcomes any barrier of both human and computerized elements is Uniquid. Uniquid considers the verification of gadgets, cloud administrations, and individuals. Uniquid plans to give character and access the board of associated things, just as people, using biometric data for the last mentioned.

6.5 Proprietorship Rights

Another significant part of the personality is proprietorship rights. The solid agreement security offered by blockchain without the requirement for a focal guaranteeing authority renders it especially appropriate for the confirmation of proprietorship rights. This incorporates advanced property, licensed innovation, and physical property, including physical items and land. For instance, Ascribe is a startup in this space. It portrays itself as an "essentially better approach to secure attribution and safely offer and follow where advanced work spreads." Credit makes a perpetual and rugged connection between the maker and their imaginative work. By permitting proprietorship to be everlastingly confirmed and followed, Ascribe influences blockchain innovation to cause it conceivable to move, cosign, or credit computerized manifestations like physical bits of work. By forestalling unapproved access to inventive work, Ascribe likewise assists makers with adapting their work.

6.6 Smart Property

The overall idea of smart property is the thought of executing all property in blockchain-based models. The property could be physical-world hard resources, like a home, vehicle, bike, or PC, or immaterial resources, for example, stock offers, reservations, or copyrights (e.g., books, music, delineations, and advanced compelling artwork).

The key thought of the shrewd property is controlling possession and access to advantage by having it enlisted as a computerized resource on the blockchain and approaching the private key. Cell phones could open after reaffirming a client's advanced personality encoded in the blockchain. The entryways of physical property, for example, vehicles and homes, could be "shrewd issue" empowered through implanted innovation (e.g., programming code, sensors, QR codes, NFC labels, iBeacons, Wi-Fi get to, and so on.) with the goal that entrance could be controlled progressively.

6.7 Security Issues and Future Directions

One focal test with the basic Bitcoin innovation is scaling up from the current greatest constraint of 7 exchanges for every second (the VISA charge card preparing system routinely handles 2000 exchanges for each second and can oblige top volumes of 10,000 exchanges for each second), particularly if there were to be the standard appropriation of Bitcoin. A portion of different issues incorporates expanding the square size, tending to blockchain swell, countering weakness to 51% mining assaults, and actualizing hard forks (changes that are not in reverse perfect) to the code.

6.8 51 Percent Attack

There are some potential security issues with the Bitcoin blockchain. The most troubling is the chance of a 51 percent assault, in which one mining substance could get control of the blockchain and twofold spend recently executed coins into his record. The issue is the centralization inclination in mining where the opposition to record new exchange obstructs in the blockchain has implied that solitary a couple of huge mining pools control most of the exchange recording. At present, the motivation is for them to be acceptable players, and a few (like Ghash.io) have expressed that they would not assume control over the system in a 51 percent assault; however, the system is uncertain. Twofold spending may likewise still be conceivable in different manners – for instance, ridiculing clients to resend exchanges and permitting noxious coders to twofold spend coins. Another security issue is that the current

cryptography standard that Bitcoin utilizes, elliptic curve cryptography, may be crackable as ahead of schedule as 2015. In any case, budgetary cryptography specialists have proposed possible moves up to address this shortcoming.

6.9 Similarity

Another huge specialized test and necessity are that a full biological system of attachment and play arrangements is created to give the whole worth chain of administration conveyance. In a perfect world, the blockchain business would grow comparatively to the distributed computing model, for which standard framework segments – like cloud workers and transport frameworks – were characterized and actualized rapidly toward the start to permit the business to concentrate on the more significant level of creating esteem included administrations rather than the center foundation. That way, the blockchain business' advancement can be rushed, without each new business rehashing an already solved problem.

6.10 The Need of a Decentralized Storage

There is a requirement for a decentralized biological system encompassing the blockchain itself for full-arrangement activities. On account of record serving, the IPFS venture has proposed an intriguing procedure for decentralized secure document serving. IPFS represents the InterPlanetary File System, which alludes to the requirement for a worldwide and for all-time available file system to determine the issue of the broken site which connects to records. In the region of filing, a full environment would likewise fundamentally incorporate life span provisioning and end-of-item life making arrangements for blockchains. A blockchain chronicled framework like the Internet Archive and the Wayback Machine to store blockchains is required. Not exclusively should blockchain record exchanges be protected; however, we additionally need methods for recouping and controlling recently recorded blockchain resources at later dates.

References

1. W.H. Hutt, The concept of consumers' sovereignty. Econ. J. **50**(197), 66–77 (1940) (ISSN 00130133, 14680297) http://www.jstor.org/stable/2225739
2. G.A. Akerlof, The market for "lemons": quality uncertainty and the market mechanism. Q. J. Econ. **84**(3), 488–500 (1970) (ISSN 00335533, 15314650)
3. M.M. Aung, Y.S. Chang, Traceability in a food supply chain: safety and quality perspectives. Food Control **39**, 172–184 (2014). https://doi.org/10.1016/j.foodcont.2013.11.007. (ISSN: 0956-7135)

4. A. Awaysheh, R.D. Klassen, The impact of supply chain structure on the use of supplier socially responsible practices. Int. J. Oper. Prod. Manage. **30**(12), 1246–1268 (2010). https://doi.org/10.1108/01443571011094253
5. C. Coff, M. Korthals, D. Barling, Ethical traceability and informed food choice, in *Ethical Traceability and Communicating Food*, ed. by C. Coff, D. Barling, M. Korthals, T. Nielsen, (Springer Netherlands, Dordrecht, ISBN: 978-1-4020-8524-6, 2008), pp. 1–18. https://doi.org/10.1007/978-1-4020-8524-6_1
6. S. Brody, H. Grover, A. Vedlitz, Examining the willingness of americans to alter behaviour to mitigate climate change. Clim. Policy **12**(1), 1–22 (2012). https://doi.org/10.1080/14693062.2011.579261
7. L. Lim-Camacho, A. Ariyawardana, G.K. Lewis, S.J. Crimp, S. Somogyi, B. Ridoutt, S.M. Howden, Climate adaptation of food value chains: the implications of varying consumer acceptance. Reg. Environ. Change J. **17**(1), 93–103 (2017). https://doi.org/10.1007/s10113-016-0976-5. (ISSN: 1436-378X)
8. B.L. Buhr et al., Traceability and information technology in the meat supply chain: implications for firm organization and market structure. J. Food Dist. Res. **34**(3), 13–26 (2003)
9. M.P.M. Meuwissen, A.G.J. Velthuis, H. Hogeveen, R.B.M. Huirne, et al., Traceability and certification in meat supply chains. J. Agribusiness **21**(2), 167–182 (2003)
10. W. Verbeke, Market differentiation potential of country-of-origin, quality and traceability labeling. Estey Centre J. Int. Law Trade Policy **10**(1), 20–35 (2009) Copyright – (c) Copyright 2009 The Estey Journal of International Law and Trade Policy; Last updated – 2010-06-20; SubjectsTermNotLitGenreText – Europe
11. M. Balcilar, Z. Ozdemir, The export-output growth nexus in Japan: a bootstrap rolling window approach. Empir. Econ. **44**, 639–660 (2013)
12. M. Balcilar, Z.A. Ozdemir, Y. Arslanturk, Economic growth and energy consumption causal nexus viewed through a bootstrap rolling window. Energy Econ. **32**(6), 1398–1410 (2010)
13. M.E. Bildirici, M.M. Badur, The effects of oil and gasoline prices on confidence and stock return of the energy companies for Turkey and the US. Energy **173**, 1234–1241 (2019)
14. J. Bouoiyour, R. Selmi, M.E. Wohar, Safe havens in the face of presidential election uncertainty: A comparison between bitcoin, oil and precious metals. Appl. Econ. **51**(57), 6076–6088 (2019)
15. E. Bouri, R. Gupta, Predicting Bitcoin returns: comparing the roles of newspaper- and internet search-based measures of uncertainty. Finance Res. Lett. (2019) 101398 Published Online
16. E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg, Tumblebit: an untrusted bitcoin-compatible anonymous payment hub, in *Network and Distributed System Security Symposium*, (2017)
17. G. Maxwell, Coinjoin: bitcoin privacy for the real world. https://bitcointalk.org/index.php?topic1/4279249.0, 2013
18. T. Ruffing, P. Moreno-Sanchez, A. Kate, Coinshuffle: practical decentralized coin mixing for bitcoin. In: *European Symposium on Research in Computer Security*, Springer, 2014, pp. 345–364
19. H. Corrigan-Gibbs, B. Ford, Dissent: accountable anonymous group messaging. In: *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ACM, 2010, pp. 340–350
20. J.H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, K. Wehrle, Coinparty: secure multi-party mixing of bitcoins. In: *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy,* ACM, 2015, pp. 75–86
21. D. Chaum, The dining cryptographers problem: Unconditional sender and recipient untraceability. J. Cryptol. **1**(1), 65–75 (1988)
22. P. Golle, A. Juels, Dining cryptographers revisited. In: *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2004, pp. 456–473
23. T. Ruffing, P. Moreno-Sanchez, A. Kate, P2p mixing and unlinkable bitcoin transactions. In: NDSS, 2017, pp. 511–532

24. R.L. Rivest, A. Shamir, Y. Tauman, How to leak a secret. In: *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2001, pp. 552–565
25. E. Bresson, J. Stern, M. Szydlo, Threshold ring signatures and applications to ad- hoc groups. In: *Annual International Cryptology Conference*, Springer, 2002, pp. 465–480
26. N. Van Saberhagen, Cryptonote v 2.0. https://static.coinpaprika.com/storage/cdn/whitepapers/1611.pdf, 2013
27. E. Fujisaki, K. Suzuki, Traceable ring signature. In: *International Workshop on Public Key Cryptography*, Springer, 2007, pp. 181–200
28. S. Noether, Ring signature confidential transactions for monero, IACR Cryptol. ePrint Archiv. (2015) 1098, 2015
29. G. Maxwell, Confidential Transactions. Accessed 09/05/2016
30. M. Mo€ser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, et al., An empirical analysis of traceability in the monero blockchain. Proc. Privacy Enhanc. Technol. **3**, 143–163 (2018)
31. S.-F. Sun, M.H. Au, J.K. Liu, T.H. Yuen, Ringct 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero. In: *European Symposium on Research in Computer Security*, Springer, 2017, pp. 456–474
32. T.H. Yuen, S.-F. Sun, J.K. Liu, M.H. Au, M.F. Esgin, Q. Zhang, D. Gu, Ringct 3.0 for blockchain confidential transaction: shorter size and stronger security. Tech. Rep., Cryptology ePrint Archive (2019). Report 2019/508. (2019). Error! Hyperlink reference not valid.
33. S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**(1), 186–208 (1989)
34. I. Miers, C. Garman, M. Green, A.D. Rubin, Zerocoin: anonymous distributed e-cash from bitcoin. In: *IEEE Symposium on Security and Privacy*, IEEE, 2013, pp. 397–411, 2013
35. R. Cramer, I. Damgård, B. Schoenmakers, Proofs of partial knowledge and simplified design of witness hiding protocols. In: *Annual International Cryptology Conference*, Springer, 1994, pp. 174–187
36. E. Androulaki, G.O. Karame, Hiding transaction amounts and balances in bitcoin. In: *International Conference on Trust and Trustworthy Computing*, Springer, 2014, pp. 161–178
37. E.B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash: decentralized anonymous payments from bitcoin. In: *IEEE Symposium on Security and Privacy*, IEEE, 2014, pp. 459–474, 2014
38. E. Ben-Sasson, A. Chiesa, D. Genkin, E. Tromer, M. Virza, Snarks for c: verifying program executions succinctly and in zero knowledge. In: *Annual Cryptology Conference*, Springer, 2013, pp. 90–108
39. B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell, Bulletproofs: short proofs for confidential transactions and more. In: *IEEE Symposium on Security and Privacy (SP)*, IEEE, 2018, pp. 315–334, 2018
40. A. Jivanyan, Lelantus: Towards confidentiality and anonymity of blockchain transactions from standard assumptions. IACR Cryptol. ePrint Archiv. **373**, 2019 (2019)
41. A. Bünz, S. Agrawal, M. Zamani, D. Boneh, Zether: Towards privacy in a smart contract world. IACR Cryptol. ePrint Archiv. **191**, 2019 (2019)
42. J. Spilman, Anti dos for tx replacement. https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002417.html, 2013
43. M. Green, I. Miers, Bolt: anonymous payment channels for decentralized currencies. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2017, pp. 473–489
44. J. Camenisch, S. Hohenberger, A. Lysyanskaya, Compact e-cash. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2005, pp. 302–321
45. G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, S. Ravi, Concurrency and privacy with payment-channel networks. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2017, pp. 455–471

46. Giacomelli, J. Madsen, C. Orlandi, Zkboo: faster zero-knowledge for Boolean circuits. In: 25th {USENIX} Security Symposium ({USENIX} Security 16), 2016, pp. 1069–1083
47. A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk, The blockchain model of cryptography and privacy-preserving smart contracts. In: *IEEE Symposium on Security and Privacy, SP*, 2016, pp. 839–858. IEEE, 2016
48. R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, J. Xie, Shadoweth: Private smart contract on public blockchain. J. Comput. Sci. Technol. **33**(3), 542–556 (2018)
49. R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, A. Juels, A. Miller, D. Song, Ekiden: a platform for confidentiality-preserving, trustworthy, and performant smart contracts. In: *IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2019, pp. 185–200, 2019
50. H. Kalodner, S. Goldfeder, X. Chen, S.M. Weinberg, E.W. Felten, Arbitrum: scalable, private smart contracts. In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 1353–1370
51. M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, et al., Meltdown: reading kernel memory from user space. In: *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 973–990
52. P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, et al., Spectre attacks: exploiting speculative execution. In: *IEEE Symposium on Security and Privacy (SP)*, IEEE, 2019, pp. 1–19, 2019
53. J. Tavares, T. Oliveira, Electronic health record patient portal adoption by health care consumers: an acceptance model and survey. J. Med. Internet Res. **18**(3), 1–17 (2016). https://doi.org/10.2196/jmir.5069
54. S. Taylor, P.A. Todd, Understanding information technology usage: a test of competing models. Inform. Syst. Res. **6**(2), 144–176 (1995). https://doi.org/10.1287/isre.6.2.144
55. V. Venkatesh, F.D. Davis, A theoretical extension of the technology acceptance model: Four longitudinal field studies. Manag. Sci. **46**(2), 186–204 (2000). https://doi.org/10.1287/mnsc.46.2.186.11926
56. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
57. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195
58. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. Blockchain, Big Data and Machine Learning: Trends and Applications, 97 (2020)
59. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global), pp. 165–177
60. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, 2020)

Review of Cryptocurrencies Implementations in the Cloud Environment: Ethereum in the Cloud

Aicha Bouichou, Soufiane Mezroui, and Ahmed El Oualkadi

Abstract All organizations desire to adopt blockchain for their structure due to the degree of security it provides and due to the success it had in the economic industry when it introduces the Bitcoin and after Ethereum. It's crystal clear that the blockchain technology is a robust technology against many of the attack attempts but still has some gray area for discussion and challenges.

In this chapter, the Ethereum blockchain description will be provided in the first place, and then we will be going around the types of blockchain and which one to adapt for each case. The third section will be about the integration of cloud and blockchain where we are going to detail the benefits and vulnerabilities of the integration and present an example for Azure blockchain. In the end, we will be presenting a simulation of the 51% attack.

Keywords Blockchain · Cryptocurrency · Bitcoin · Ethereum · Cloud · Security

The original version of this chapter was revised. The correction to this chapter is available at https://doi.org/10.1007/978-3-030-70501-5_15

A. Bouichou (✉) · S. Mezroui · A. El Oualkadi
Laboratory of Information and Communication Technologies (LabTIC) Ecole Nationale des Sciences Appliquées de Tanger Abdelmalek Essaadi University, Tétouan, Morocco
e-mail: aicha.bouichou@etu.uae.ac.ma

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_5

1 Introduction

In our days, where everything is being digitalized, money cannot be out of the reach of digitalization since it is a concept that can have many forms.

In addition to the many problems that were there because of the centralization, the cryptocurrency exists to face them all. Many people and systems tried to implement some solutions, but it was an idea and a huge investment in time and knowledge to make it happen.

The first principle of cryptocurrency digitalization is also traced back to "bit gold" which Nick Szabo worked on between 1998 and 2005 but was never implemented. Bit gold is the primary Bitcoin precursor.

The b-money of Wei Dai (a conceptual framework published in 1998, cited by Satoshi in the Bitcoin white paper) and "egold" (a centralized digital currency that began in 1996) are all notable early references.

With that history noted, modern digital currency started in 2008 with the release of Satoshi Nakamoto's paper [1] (an anonymous individual and/or group) where they detailed what would become blockchain and Bitcoin.

When it was founded in 2008, Bitcoin became the predominant decentralized digital coin. In 2009, it then went public.

Bitcoin is the most popular cryptocurrency as of 2019. Other coins, such as Ethereum (ETH), Ripple (XRP), Litecoin (LTC), and more, are also notable.

There have been over 500 different forms of cryptocurrencies for online trading markets as of January 2015. Just ten of them, however, had market capitalizations of over $10 million.

This chapter reports on the evaluation of the cryptocurrency the Ethereum, where we are going to discuss its basics and features and give an analysis of the attacks that happened or can happen in its network, besides of discussing its implementations in the cloud paradigm.

The chapter contains six sections: the first one contains this introduction, and the second section deals with the basics of the Ethereum. The third section tackles the decision-making of which type of blockchain to adapt for each use case. The fourth section is about the combination cloud blockchain, where we detailed the benefits, vulnerabilities, and challenges of integration of blockchain into Cloud or vice versa, we introduce an implementation of the 51% attack in the fifth section, and the sixth section is for the conclusion.

2 Related Works

As we have mentioned in this chapter, the blockchain paradigm starting from the white paper of Satoshi Nakamoto has brought the world to a new digital era by providing a secure and reliable system for trading and making it available for everyone around the globe. Eliminating the centralization was the main motivation for the migration of

other paradigms such as Cloud and Cloud of Things to the blockchain technology. *Vitalik Buterin* brought new dimensions to the paradigm by adding features related to automatization and introducing new algorithms for incentives like PoS, which opened the door to most new technologies to adapt and make use of blockchain benefits.

The works we have reviewed in this chapter are divided into two categories: works relating to the security and efficiency of smart contracts work regarding cloud implementation of blockchain.

Work Related to the Implementation of Blockchain into Cloud

"Blockchain-based fair payment smart contract for public cloud storage auditing" has presented a non-interactive, publicly proven data ownership scheme and efficient construction design. "Building Logistics Block Chain Platform Based on Cloud Computing" [2] paper tackles the data provenance issue by adopting the blockchain into logistic. The logistics blockchain and cloud distributed storage form a consensus algorithm that allows logistic transactions to be decentralized, data encrypted, secure, and immutable, which can be tracked back to the source of each cargo and the entire logistics transportation method. [3] offered a thorough debate on principles, motives, and architectures with a systematic analysis of the convergence of blockchain and the Cloud of Things (BCoT). In the state-of-the-art survey on BCoT applications, BCoT platforms are presented with challenges and potential research directions. [4] provides a survey of IoT blockchain protocols, analysis problems, and IoT-blockchain integration issues. [5] introduces a systematic survey of the fundamental principles of blockchain, architectures, and IoT applications. [6] is about IoT blockchain use, while [7] has conducted a study of the cloud computing blockchain and its cloud-based security solutions. In [8], an implementation of blockchain for cloud systems with relevant problems was conducted, and a systematic survey of the combination of blockchain and edge computing [9] was conducted.

For the works related to the correctness of the smart contract, this chapter has focused on the Azure workbench as an example of the implementation of Ethereum blockchain into the cloud so we have two important papers to mention: first is "Formal Specification and Verification of Smart Contracts in Azure Blockchain," which represents the tool *VeriSol* that helps verify the correctness over the Azure blockchain of smart contracts, and second work is "Formal Verification of Workflow Policies for Smart Contracts in Azure Blockchain," which represents some "best practice" to deploy smart contracts over the Azure workbench and offers verification and study of the *VeriSol*.

3 Description of the Ethereum Blockchain

Ethereum is a derivation from Bitcoin. The term Ethereum refers to three things [10, 11].

Ethereum network: As all open-source blockchain networks, Ethereum is a kit that allows us to create the software economic structure, along with account

management and its necessary exchange unit that is the coins or tokens that are no different from any tokens in any system. Ethereum takes the concept of blockchain to another level by offering the ability to create a financial contract called smart contracts inside the system within a few minutes.

Ethereum protocol is a set of rules in telecommunication that specifies how a device (and its programmer) can connect to, engage in, and transfer information expected by the system. Hardware, applications and plain-language instructions may be involved. The software is free and no special hardware is needed; it is designed to ensure decentralization for the applications without neglecting the security and the interactivity. The protocol's application layer, where all the user information resides, since the protocol offers a lot, is thinner.

The Ethereum project collectively funds the creation of the protocol and network together.

The Ethereum retains too much of the fundamental Bitcoin principles, but as its main feature is unique, it may be considered an entirely new network.

In what follows, we will describe some new notions and components of the blockchain: Ethereum.

3.1 Definition of Ethereum Virtual Machine (EVM)

The EVM is a worldwide device that can be used by anybody, payable in ether, for a small fee. It is a single, global 256-bit machine where all operations on each network node are local and are performed in relative synchrony. Technically, it is a machine composed of several other machines. Nodes replicate the same transactions and preserve the same state across thousands of computers (Fig. 1).

The EVM is composed of many private computers, so we can call it a *shared ownerless computer*. The aim of the ownerless configuration is to optimize the uptime and security while minimizing the subterfuge incentives.

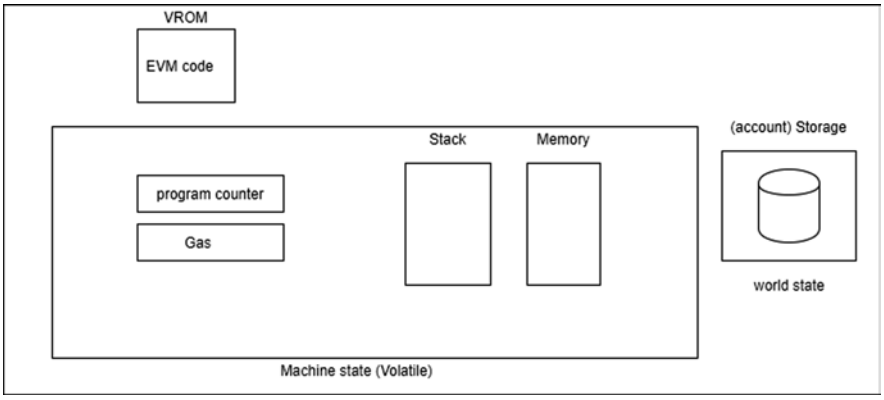


Fig. 1 The description of the EVM

A virtual machine is one massive global computer made up of consistent nodes, which are also computers themselves. It is a computer system emulation that can be produced with hardware, software, or both, by another computer system. In the scope of Ethereum, it is both.

3.1.1 The Uses of the EVM

The EVM has many uses from the different components of the Ethereum protocol:

- Run random "smart contract" programs written in Solidity, and all users have full access at no expense to the same Fedwire-like system, with the ability to program transaction-free protocols.
- The EVM is a singleton transaction machine with a shared state that functions as one big data entity.
- EVM is a runtime environment for small programs for software developers that can be
  executed by the network.

The EVM is sandboxed and interference-free and therefore isolated from other networks too, making it impossible for a group to back out of a smart contract. The EVM runs a bytecode in which smart contracts are compiled. EVM is a state machine.

Putting All Together
The EVM can be defined as a collective emulation runs on thousands of computers that can run any of hundreds of versions of Windows, Linux, Ethos, and MacOS on individual basis.

3.1.2 The Work of the EVM

The EVM periodically runs loops at the current program register, which acts like a delicatessen queue, attempting to execute whatever instructions are.

Tasks for the Loop Are:

a. For each instruction, measure the gas cost.
b. If required, it uses memory to execute the transaction if (a) succeeds.
c. Repeat (a) and (b) until all codes are completed by the VM or an exception is thrown, the r error occurs, and the transaction is rolled back.

As time goes, the system aims to build a trustworthy history to guarantee that any future change of state is legal, not a bad actor's introduction of instructions.

The EVM purpose is to overcome the problem of *Diff matching* that can occur because the same database has multiple near-simultaneous charges from many users all around the world.

The stability and security of the EVM comes from the vast number of mining machines on the network induced by the gaining of fees denominated in Ether or Bitcoin.

3.1.3 Renting Time on the EVM

The EVM executes on each instruction to ensure that the mechanism is not jammed by meaningless spam contracts and an internal counter keeps track of the fees paid, which are credited to the user, any time an instruction executes.

The user's wallet reserves a limited portion (selected by the user) to cover these fees any time the user initiates a transaction. The network propagates the transaction around when a transaction is received, so that all the nodes will include it in the current block.

3.1.4 Gas Unit to Control the Overuse of the Resources

The gas is the work unit used to calculate how costly an Ethereum process can be in terms of computing. It is a statistic representing the number of steps to complete the instructions in the transaction that the EVM would have to take.

And if the execution fails for whatever reason, gas costs are charged with limited quantities of ether to guarantee a prepaid payout for the miners who run code and protect the network and works around the *halting problem* and guarantees that execution does not go on longer than the time it prepaid for. The gas is not a subcurrency; you cannot hold or hoard it. And there is no gas token.

In order to distinguish the computing price from the very unpredictable price of the ether token, the gas plays a significant role, since payments in the EVM are dependent on the amount of work being performed, not on the scale of the contract, since Solidity code can be extremely complex and can produce a lot of computational work, while a long code can generate less. The customer must pay for the machine effort, and the EVM will expend each contract running, thereby minimizing the risk of running expensive never-ending programs.

The transaction sender must include a quota on gas, indicating how much the user is willing to pay for the execution of his transaction. Both steps are rolled back if the cumulative number of steps approaches the gas budgeted for a transaction, and no portion of the transaction is performed.

Scaling is done by the gas fee program in a de facto manner. Miners are free to pick the transactions paying the highest fee prices and may jointly choose the block gas limit as well.

The gas limit defines how much measurement (and how much storage can be allocated) can take place per block; this offers:

- The flexibility of the EVM computation price
- Responsive to requirements (user)

- Costs incurred by the miners who do the substantial job of handling transactions
- Hardware repair
- Paying electricity bills

3.2 The Communication Between the Decentralized Applications (Dapp) and the EVM

The distributed app (Dapp) describes a web- or smartphone-accessible front-end that uses the EVM as the back-end GUI framework that will rely on several smart contracts [12].

So to speak, *Dapp* is composed of smart contracts that they are executed at about the same time by nodes on the Ethereum network.

In practice, it is like globally accessible web services running on the EVM but made available to users via a standard front-end of HTML/CSS/JavaScript that they can access through their web browser or a mobile app or an Ethereum browser such as Mist [13].

In other contracts, Dapp can be able to call up a certain public feature to make use of its capabilities. Data interchange formats are like international postal services, but they can run multiple QoS or languages and they may share information with a server that is not like them at any stage. Programmers engineer their systems to submit information about other programs in notations to get the translation right, which defines a format for an entire object.

Remark
The smart contract is the functionality module you upload to the EVM.

3.2.1 Whisper Protocol/Web3

Whisper is a protocol for private messaging which is part of the large Ethereum protocol. It is a distributed messaging system that is part of the protocol of Ethereum that will be open to web developers using the EVM for their back-end (Fig. 2).

Web-based JavaScript code transfers JSON (JavaScript Object Notation) details that may include numbers, lists, and organized sequences of values for such attributes. The two JSON-equivalent Web3.js data objects, called JSON-RPC objects, are:

Web3.eth: is used primarily for connections with blockchains
Web3.shh: is specifically found in Whisper

For the decentralized network, Web3 is a general concept, it is very much a vision based on Ethereum protocol, and it is commonly known to have three components:

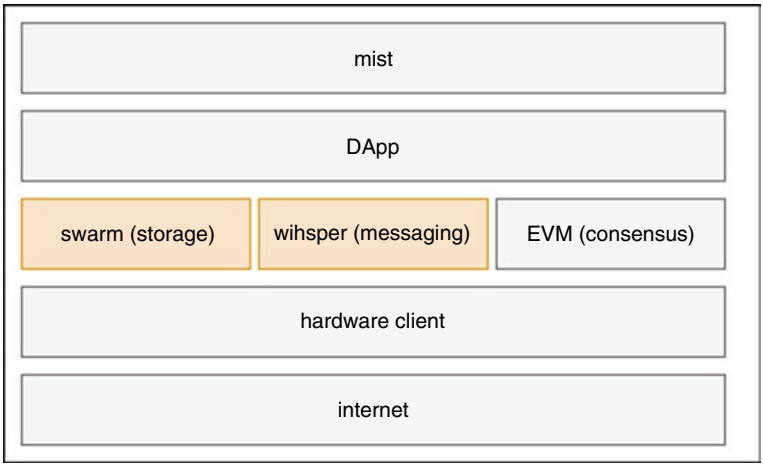


Fig. 2 The integration of Swarm and Whisper

- Identity and messaging framework for P2P
- Shared state (blockchain)
- Decentralized storage of files

There are no web servers, no caches, no reverse proxies, no load balancers, no content distribution networks (CDNs), or other vestiges of legacy large-scale implementation of web apps in the web3 model, and even the DNS is free.

3.2.2 The Domain Path (Swarm)

Swarm is an accounting protocol content addressed. It runs with persistent data, exchanging it and storing it in ways that make it easy to remember when an application wants it across a distributed network. Swarm's goal is to be able to locate multiple copies of a file under the same memory address, mimicking domain paths with their folder layout in today's URLs. It should be mentioned that this addressing protocol is hardware agnostic.

It merely serves the function of an index, where [14, 15] chunks of data are stored. This scenario of blob storage is a common application for decentralized systems, and with some of the developments pioneered by BitTorrent, Swarm will make it even easier. Here is how the method of data retrieval using the Swarm protocol will operate with a Dapp:

1. Navigate to the app in the Mist. Enter an Ethereum domain name.
2. The domain is translated into a Swarm hash.
3. Swarm retrieves HTML/CSS/JS files linked to this hash.

The experience will not be any different for consumers from the use of an existing web application.

The aim here, however, is to achieve P2P storage that is resistant to distributed denial of service (DDoS) and provides 100 percent uptime and can be programmatically accessed conveniently by all kinds of users, accessing files on all different storage networks.

So*, the application of Ethereum scales horizontally the way you would like to scale a cloud application*.

3.3 Mining in the Ethereum Blockchain

Mining is the method by which machines enter the network and start validating transactions. Electricity is absorbed by this operation, and so miners are paid a reward. Mining nodes allow a consensus on the order of transactions to be reached. It achieves the consensus needed to make valid improvements to state.

The transition function of the Ethereum state can be described as the six steps below:

(a) Check the format of the transaction (right number of values, a valid signature, nonce matching) if anything is missing; it throws error.
(b) Calculate the transaction fee by the price of STARTGAS*gas (STARTGAS is the amount of work needed) and subtract the fee from the balance of the user's account and raise the amount of work required by the sender. If the ether is not available in the account, return error.
(c) Initialize the charge for gas, take off a certain amount of gas processed in the transaction per byte.
(d) Shift the transaction's value to the receiving account. Build it if the receiving account does not exist yet. (Until a transaction takes place, the network cannot hear of a given address.) If a contract address is the receiving address, run the code of the contract before the code finishes execution or the gas payment runs out (smart contract execution).
(e) These transaction modifications are rolled back if the sending account does not have enough ether to complete the transaction or gas runs out. Caveats are the fees that still go to the miner and are not refunded.
(f) If the transaction triggers an error for some other reason, refund the gas to the sender, and give the miner any fees related to the gas used.

Remark
Using more STARTGAS will not cause the transaction to be processed faster and may make the transaction less desirable to miners in some cases.

3.3.1 DAG File

The defense against optimizing mining hardware is the Ethash algorithm. It is a Dagger-Hashimoto derivative, which is a memory-hard algorithm that cannot be brute-forced with a custom app-specific integrated circuit (ASIC). Its toughness on a directed acyclic graph (DAG) file is the secret to this memory hardness algorithm. A technical term for a tree in which each node is permitted to have multiple parents within ten levels, including the root, and a total of up to 225 values, which is a 1GB dataset, has created a new tree every 125 hours, or 30,000 blocks, equal to an epoch. The DAG file levels up the miners' playing field; meanwhile, it allows cluster block times around the 15 sec mark by ensuring that you cannot guess the correct once a whole lot faster than your rivals even with huge computing resources.

3.3.2 Proof of Work

Mining devotes computational effort to strengthening the right version of a given version of history. This includes the implementation of a memory-intensive hashing algorithm known as a proof of work algorithm (for the Ethereum protocol is *Ethash*).

Ethash is a new feature developed by the core developers to fix the issue of centralization of mining evident in Bitcoin. It is like the consensus algorithm of the Ethereum: consensus engine.

The one chosen as canonical is the block with the largest amount of proof of work behind it. Hash power is defined as the amount of computation that a miner can add to the network. Hash power represents the components and requirements of an individual device – the power supply, the speed, power, and quality of graphics processing cards, and sufficient voltage availability.

When more hash power is added, the cryptographic proof which results from mining can be completed more quickly. Thus, miners from the "mining pool" are increasing their chances of winning prizes, which can be divided among the group.

A fork state occurs when nodes disagree about which root-to-leaf path is the real blockchain; this is analogous to the EVM splitting into two EVMs.

Miners' time is a consideration for the new cryptocurrency, they race to turn on their machines because there are:

- Less competition for early-day fees, which is a chance to earn more.
- Tokens belonging to helpful crypto networks typically inflate throughout their lifetime in price. Therefore, winning them faster provides more chances to benefit from appreciation.

3.3.3 Difficulty

Ethereum is a self-regulating network; a dynamically self-adjusting value called *difficulty* will increase to remain within range of its ideal 15-sec block time.

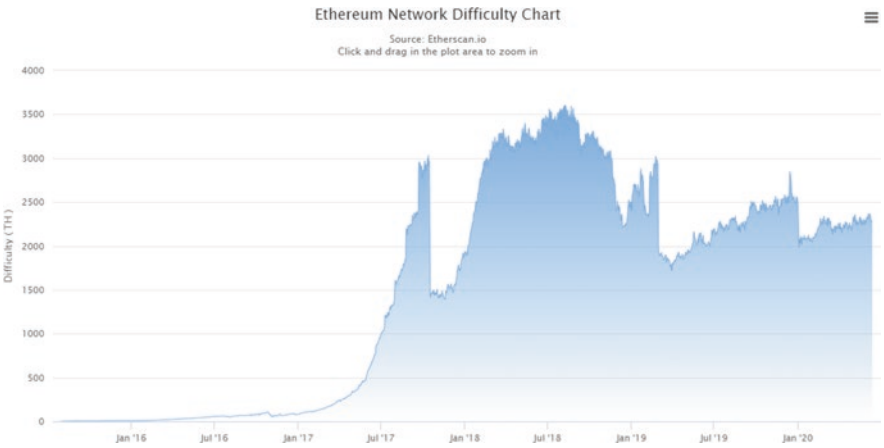


Fig. 3 The Ethereum difficulty

This value is balanced by the velocity frequency to locate the blocks. When time passes, network complexity grows. With a formula, this value is determined. This variable of difficulty (Fig. 3) can be viewed as part of the incentive system to bring miners to the network as soon as possible and remain there.

The others use it to assess the score of a block that is sometimes referred to as its heaviness. It can be said that the longest, or highest scoring, route through the transaction data structure is the longest, the one that most miners have typically converged on as the real root-to-leaf direction, *the canonical one* (Fig. 4).

The winning block earns flat payment, transaction fees, and shares of the bounty of all uncles who helped it win.

To make block history "forgettable" is assured by requiring uncles to be within seven blocks of the winning block to earn a partial award after a limited number of blocks.

It must pass a long series of steps used in the processing of each block for the nephew; true block, to escape unclehood and be the heaviest block, and the block validation algorithm are most important; validate the hash in the header of the block. These steps produce a canonized block.

The steps in order are the following:

(a) Verify if the referenced previous block exists and is correct.
(b) Verify that the block time stamp is greater than that of the previous block referred to and less than 15 minutes in the future.
(c) Check the validity of the block number, difficulty, transaction root, uncle root, and gas limit (various Ethereum-specific low-level concepts).
(d) Check that the nonce is correct on the block, showing proof of work.
(e) Add all transactions to the EVM state in this now-validated block. If any errors are made, or if the total gas exceeds the GASLIMIT, return the error and return the change of state.

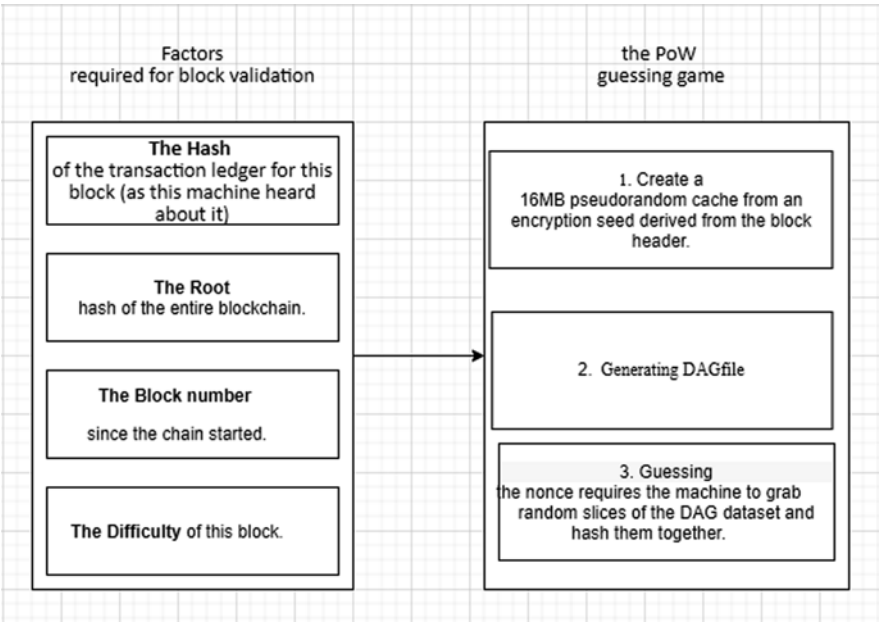


Fig. 4 The process for the block validation

(f) Apply the block reward to the final state.
(g) Verify that the final state of the Merkle tree root is equal to the root of the last state in the block header.

3.3.4 Patricia Tree/State Tree

Ethereum implements a data structure reflecting the state of the EVM, known as the Patricia tree, which is the Merkle Patricia tree that includes a cryptographically validated data structure that can be used to store all (key, value) bindings. It is totally deterministic, ensuring that a Patricia tree with the same bindings (key, value) is guaranteed to be the same down to the last byte and thus has the same root hash, offers inserts, lookups, and deletes with the holy grail of O(log(n)) quality, and is much easier to grasp and code than more difficult comparison-based alternatives such as a red-black tree. An Ethereum block header contains three types of trees:

- Transaction tree; Merkle structure
- Tree receipts (data showing the outcome of each transaction)
- Tree of state

3.4 Account

An account is a data object, an entry indexed by its address in the blockchain ledger, containing data on the status of that account, such as its balance. The account does not store any personal information. And one person can have as many accounts as he would like. The account address is exactly the public key – that is not memorable – that has a matching private key; it is how the user accesses his accounts. Technically, the address is the hash of the public key; we disregard this technical differentiation for convenience.

The accounts are represented as in Bitcoin, with a hexadecimal address. There are two types of accounts:

Externally held accounts: EOA is often referred to as an account operated by a pair of private keys that an individual or an external server can possess. The EVM code does not keep them. Their features are the following:

- Contains an ether equilibrium
- Worthy of sending transactions
- Regulated by the private keys of an account
- Has no related code
- The database of key/values found in each account, where keys and values are both 32-byte strings

Contract accounts: They are not handled by humans; they store instructions which are enabled by foreign accounts or other contract accounts. Their features are the following:

- Have an ether balance.
- Hold some contract code in memory.
- Can be triggered by humans (sending transactions) or other contracts sending messages.
- When executed, can perform complex operations.
- Have their persistent state and can call other contracts.
- Have no owner after being released to the EVM.
- Each account includes a key/value dictionary, where the keys and values are all 32-byte strings.

3.5 Transactions

Transactions are a means for an external account to send orders to the EVM to execute such procedures; otherwise, it is a way to bring a request into the system for an external account. An EVM transaction is a cryptographically signed data packet that stores a message asking the EVM to move the ether, create a new contract, activate an existing one, or perform a calculation. A transaction is like a private

connection between two users on an unsecured network, which may still transfer value to each other; we can talk here about encrypted communications.

The characteristics of transactions:

- Recipient address, the method for uploading smart contracts is to specify no address recipients (and append smart contract data). The address of the contract is returned so that the customer knows in the future when to use this contract.
- A signature representing the sender.
- A value field for the sum received, optional field if this is being sent to a contract address.
- A STARTGAS, the maximum number of prepaid computational steps in the transactions.
- GASPRICE, the fee that the sender prepared to pay for gas.

Remark
The contract address can be the recipients of transactions.

3.6 Messages

A message is a chunk of data. For programmers, it is a call to function.

The characteristics of messages:

- A message is sent to another contract by a contract (never to or from a person), which are virtual objects that are never serialized and only exist in the EVM.
- Paying a miner on the Ethereum network is achieved by means of a message to raise the payment address of the miner, not a purchase.
- The message is transmitted while the EVM is running a contract, and the CALL or DELEGATECALL opcodes are executed.

The message includes the following:

- The address of the sender
- The address of the receiver
- Sent value
- The optional area of data (input data for the transaction)
- The STARTGAS

3.7 Other Aspects

Ether balance can be queried by every device running a wallet or Ethereum node. Even if the device where the Mist wallet gets destroyed, the user needs only his private key to access his ether from a new node. Anyone with your private key is called YOU by the EVM because it is a global computer that has no idea about the

node you are going to use. There is no way that your private key can be backed up. The EVM is a closed system, which means that it is when another account has sent a payment that an account raises and thereby decreases the same amount.

3.8 Smart Contracts

The Ethereum network enables anybody to write a contract that transfers ether in the future that is trustworthy and self-executing. This offers the contracting owners a justification for keeping and using ether as a store value.

According to Gresham's law, in an economy, "bad" money drives out "good," meaning people invest or store money they intend to appreciate while spending money they expect to depreciate.

In addition to conventional use, transfer value, and purchasing of goods and services, the Ethereum has another use that pays to run programs on the Ethereum network that can pass Ether now or in the future or when certain conditions are met such that applications and services can be considered a commodity such as fuel for the network to run. So, it has an added inherent value factor above Bitcoin.

For the smart contract, they are some business logic operating on the network, transferring value semi-autonomously, and imposing payment arrangements between sides; they are more like the notion of object-oriented programming classes.

Data is encoded but not encrypted inside smart contracts themselves. Encryption is for hashing massive datasets and checking senders and receivers of transactions only.

Smart contracts are an arrangement between accounts in Ethereum to allow a transfer of ether (payment) until such conditions are met, so they are empowered to keep assets in escrow and move them until the contract terms are fulfilled.

Tokens are only one smart contract functionality application on the EVM. Within the Mist wallet, developers have placed easy-to-use models to launch your tokens easily. They are only important when they assume they can be used by the community.

Seven ways of thinking about a smart contract are available:

- Maintaining an accounting structure in the real world or any contracts on something.
- Creation of forwarding contracts, such as bank account that immediately resends profits to a different bucket.
- Manage a contract, such as a freelancer deal or payroll, with multiple people.
- Act as a program library with other agreements.
- Act as controllers for other contract schemes or packages.
- Serve for a communal online service as app-specific rationale.
- Serve as a utility that users can use, such as a random number generator, on a single-serving basis.

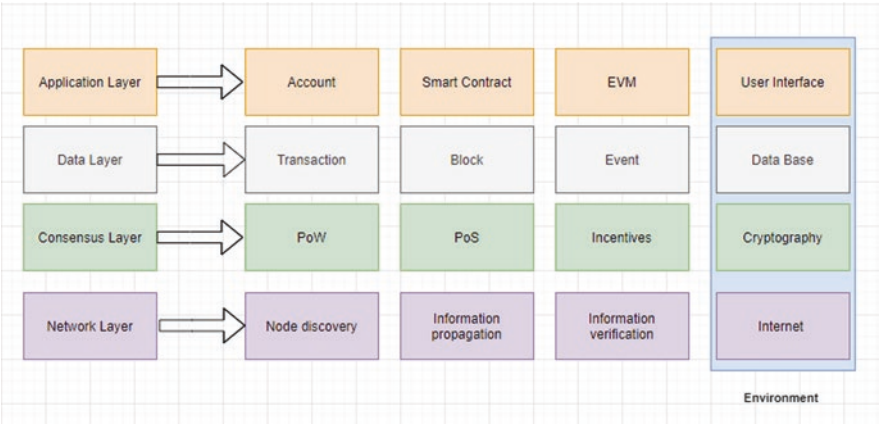


Fig. 5 The Ethereum blockchain architecture

Remark
The Mist browser is the native Ethereum browser that holds ether, and it is a tool to start prototyping smart contracts with just the Solidity scripts.

Putting All Together
Figure 5 represents the general architecture of the Ethereum blockchain and its different layers.

3.9 Crypto Economics and Attacks

To render some attack vectors, the Ethereum network utilizes economic incentives and disincentives. Fees fall under the disincentive category; it makes sense to bring in place a processing fee to discourage pranksters from wasting the capacity of the network. Blocks with massive quantities of gas are a major risk. It takes a long time to spread, but the protocol is built to cut off late blocks using different methodologies and set a floating limit on the process.

The architecture of software systems with rules of game theory constitutes the new concept of crypto economics in which the incentives and disincentives are carried over to secure the system.

Crypto economics is the study of economic behavior carried out through secure computing networks. It is a scheme of economic incentives and disincentives that overlaps with the field of game theory, which is the study of logical, informed decision-making in conflict and partnership contexts. In economics, defense planning, and gambling studies, game theory is used as a technique for observing, evaluating, and forecasting the actions of people and computers operating within a known system.

Certainty and privacy are the main promise of information theory. Every time, we can trust machines to run the same code the same way, thereby allowing the high

degree of automation we experience today to protect the data sent through networks. With much greater power than the enigma machine circa 1945, today's computer can encrypt details.

The crypto economics area comprises the following:

- Online trust
- Online popularity
- Contact which is cryptographically protected
- Decentralized apps
- Currency or services as a web service
- Financial P2P agreements
- Consensus protocols for network databases
- Antispam and algorithms of anti-Sybil attack

Crypto economics create a game-like structure with workable incentives and disincentives which provides an equilibrium that keeps the network up and going. The network can work with other crypto network protocols according to those expectations that are predicted to be real-life experiences. The game's assumptions are the following:

Beware of centralization: Any two entities who each possess 25% of the hash power of network mining or the cryptocurrency itself are dangerously close to being able to trigger a violent fork and undermine the integrity of the network.

Most people are rational: Some of a network's quota will consist of users who operate in ways that are hard to reason about. Anybody will attempt, either on purpose or by some extraordinary mistake, to bring down the network.

Large networks have individuals that churn in and out: This causes ebbs and flows in the network traffic and usership, but some users can adhere to and sustain high activity levels.

Censorship is not possible: Contracts should be assured that they can receive absolute communications from other contracts.

Nodes can talk freely: Communication between is quick and easy.

Debt and unfavorable declarations of credibility are unenforceable: Because anyone who uses a public chain will generate a new wallet address at any moment, only private chains with limited-issue wallet addresses regulated by a software contract or central authority will have certain forms of communities.

Crypto economics includes developing a security layer between public networks and attackers of all types, incorporating game theory device architecture, cryptography, and cryptographic hashing to secure a widely used resource that is commonly used. Public chains need to be immune to attackers with vast quantities of computational resources since they are public, whereas networks of more nodes and more globally dispersed nodes, owned by discrete as compared to dower, are assumed to be safer.

By developing an *ASIC-resistant Ethash algorithm* and engineering the network to rapidly increase the complexity, the protocol designers assured that there would be no opportunity for miners to professionalize and consolidate.

3.9.1 Common Attacks

To show the utility of its specification when the network is under attack, the Ethereum White Paper uses the following examples:

- It will inevitably run out of gas if an intruder gives a miner a contract containing an infinite loop. The transaction, however, is still true in the sense that the miner will demand a fee for each cryptographic move taken by the program from the attacker.
- And if an intruder wants to pay the required gas fee to keep the miner running, the miner will see that the amount of STARTGAS is too high and will realize in advance that too many steps will be taken.
- Imagine that for his gas payment an attacker is careful: the attacker sends the contract code with just enough to make a withdrawal, but not enough to make the account balance go down. This is like a double-spend attack, generating capital from thin air. However, in Ethereum, when it runs out of gas in the process, this transaction will be absolutely rolled back.

More attacks can have a place such as [16]:

DAO 51% attacks: This attack is "buy 51% of the shares and use them to vote to give yourself 100% of the money" attack; in corporate land, this (and much more subtle versions of this) is essentially the reason why shareholder regulation exists. One possible countermeasure is to build a cooldown period to let people pile in even more money on the "good guy" side if such an attack takes place, preventing the vote from passing through and even allowing the good guys to in turn disenfranchise the attackers.

Quadratic voting: The definition is simple – by paying k^2 tokens, everyone can make k votes for a decision; it's only a plurality vote from there.

The idea is that if someone benefits x from a decision being taken, and each vote is likely to be pivotal p, then they can continue purchasing votes as long as the price of the next vote is lower than px.

Since the overall price of k votes is k^2, and we know from estimation that the derivative of k^2 is 2 k, users will have the ability to purchase tokens before 2 k > px; thus, they will buy tokens k = px/2.

From this math, you can see that the number of tokens an elector purchases should be equal to x, i.e., the sum they receive from the decision being taken.

The amount of votes an elector makes should then represent the strength of their preference and not just what choice they choose.

Bribe Attacks: A lot of DAOs on Ethereum are starting to look at voting mechanisms for decision-making. Can we bribe participants to vote in specific ways? Here's one interesting live experiment: use BTC Relay to trustless bribe Bitcoin miners to vote for the Classic fork on blocks where block number % 4 > 0 and Core otherwise (the weird bribing rule is chosen so that it doesn't affect the outcome of the decision, as the threshold for Classic is 75%, and so assuming Core and Classic miners are equally

susceptible to the bribe, it should proportionately shrink (p-0.75) (where p is the percentage of miners that vote for Classic) and not change the sign, and so that we can tell how many miners are taking the bribe and don't have to argue about whether or not they took the bribe because they wanted Classic to succeed anyway).

After we have presented the major components of the Ethereum blockchain and had a view over the security over its network, we will be presenting the types of blockchain that exists and how to make the decision to adopt this type and not the other.

4 Types of Blockchain and How to Decide Which One to Implement

All organizations are looking to adopt blockchain technology, but some criteria should be taken by consideration; for example, scalability, capacity, latency, and privacy make it appropriate for application in some environments and some not [13].

For decision-makers and device developers, choosing what type of blockchain and what kind of configurations to use poses a major challenge because each design of the blockchain needs a carefully formulated decision based on the application's characteristics. Three forms of blockchain exist:

1. *Permission-less public blockchain*: It is an open network, where all nodes can do anything, the consensus is based on POW (solving a computational problem), and based on the stack owned by various miners, the POS determines the next correct block in a deterministic manner (number of tokens).
2. *Permissioned public blockchain*: It is a closed network where only confirmed and trustworthy nodes (e.g., RIPPLE, MultiChain, Eris, and Hyperledger Fabric) can join, often called Hybrid blockchain. All nodes can access data, but transactions can be checked only by approved nodes. By using consensus-based proof of eligibility, users are allowed. If no trust problems are raised, the audibility may be the justification for choosing such type.
3. *Permissioned private blockchain*: It is a closed network, where only confirmed users can participate (e.g., Hyperledger, Corda). The consensus within the organization is a practical byzantine fault-tolerant consensus PBFT.

There are ten efficient steps to make such decision, as described by the blockchain consultants Asger B., Marten Risius, and Roman Beck [17]:

Step 1: Do we need a distributed shared database? If there is a scalability issue, we use the blockchain with a database off-chain.

Step 2: Do we have many actors in the system? Essential blockchain functionality if there is more than one actor communicating with the database?

Step 3: Do we have a conflict issue? If they are trusted, so blockchain is not necessary; if not, it is very important. Using the smart contract and the tamper-resistant character.

Step 4: Do we seek decentralization? No trusted third party.

Step 5: Do we have to configure an access policy? If they do have the same rules, using a relational database is more appropriate.

Step 6: How frequent the transacting rules change? Very difficult to perform changes in a blockchain structure because of their consensus-based procedures. So it is not advisable to use blockchain in a frequently changing transaction rules, because the smart contracts are automated.

Step 7: Is there a requirement for an objective, unchanging log? A standard ledger could be a better alternative than a blockchain as it does not need a guaranteed authenticity of transactions and does not need a conclusive authentication of transaction information such as timestamps and parties involved.

Step 8: Is public access necessary? This defines which type of blockchain: permission-less, private, and public permissioned depending on the governance system for the regulation of network access and participation. Permissioned is following the know-your-customer regulation. This means only the preregistered node can participate, while permission-less means that all nodes can participate.

Step 9: Are the transactions public?

Public: all nodes can read it (e.g., Bitcoin and Ethereum).

Private: only preregistered nodes can read it (e.g., IBM Hyperledger Fabric).

Step 10: Where is consensus determined? The answer to this question determines which mechanism of consensus is adopted.

In general, the first step to a successful implementation of a suitable blockchain to an environment is by defining the characteristics and configurations that are working with this environment.

5 The Combination Cloud Blockchain

The mixture of cryptographic structures and distributed public ledger constitutes the principal basics of the blockchain structures. This combination allows the building of every form of framework on top of the blockchain without any trust problems over the network. The same case in the blockchain-enabled cloud systems.

The shared ledger cloud potentially contains all the history of transactions in the system and facilitates the verification, monitoring, and the clearing of the assets without the involvement of cloud administrator.

So, the blockchain is beneficial to cloud in assuring the data provenance (the verification of the source of the data) and facilitating cloud auditing.

5.1 Assuring Data Provenance and Auditing Over the Cloud

Traditional data assurance relies on data protection, transparency, and availability. Assuring the provenance of the data (where the data originated from) is, however, a concern in cloud environments. It would be possible to detect insider threats, repeat test findings, and determine the precise cause of system/network intrusions if real data provenance existed in the cloud with all data collected on cloud servers, distributed data computations, data transfers, and transactions.

The provenance of data will be very beneficial in debugging system break-ins for cloud infrastructure managers. Cloud computing environments are popular for the sharing of data between multiple applications and components of the network.

To ensure resilience, multiple copies of data take different paths, which make the identification of the origin of the attack and its impact and tool very difficult for the administrators.

The usual cloud uses the logging and auditing technologies to achieve the tasks [18]. But for such a dynamic system that is founded on layers of interoperating software and hardware, spread across the globe and operational constraints, these innovations are difficult to accomplish.

Provenance management will be accomplished by collecting knowledge about the actions conducted on each cloud storage entity, and blockchain technologies can be useful to guarantee that the content is unalterable.

The blockchain is beneficial to the cloud in addressing some security issues in the cloud environment, such as assuring data provenance.

The data provenance represents many challenges to the cloud that blockchain has the power to work with:

(a) *Blockchain and Cloud Security*: Cloud infrastructure provides the customer with remote cloud storage with their own information and delivers on-demand content and utilities from a common pool of configurable computing tools.
(b) *The Security of the Outsourced Data*: It depends on the security of the cloud computing system and network. However, some of its criteria can be vulnerable, such as on-demand services, uninterrupted access to the network, pooling of resource, and fast elasticity.
(c) *Insecure Implementation*: The insecure implementation brings many disadvantages to key tools for virtualization, cryptography, and network applications for cloud computing.

We must mention that cloud computing has several challenges on behalf of the security controls, for example, key management. Good management and storing of different kinds of keys is needed to build a good and efficient key management system in the cloud computing infrastructure. The challenge here is about the diversity and heterogeneous hardware/software that runs on the virtual machines and the geographic distribution of cloud computing storage.

In the cloud infrastructure, protection of data relies on PKI-based signatures, which expresses the need for a strong attribution to the detection of unauthorized

changes to data and identifying the sources responsible for it. A centralized authority relies on the application of the PKI signature. Blockchain and keyless signatures have been suggested as a solution to this inconvenience because it provides safe information transmission via cryptographic secure keys through the distributed framework.

The source of data records information about changes made on data transferred across the system parties. The system of distributed ledgers offers a record on all modifications performed on data and shares this record with all participants, so there would be no need for a central authority.

The system of verification of transactions is made by a consensus of most participants. The data are eternal in this distributed ledger. By distinguishing the processes of defining signers and reputation security from the processes responsible for preserving the confidentiality of the keys, the keyless signature solves the issue of PKI key compromise. Cryptographic tools such as keyless cryptography and asymmetric cryptography include the mechanisms of authentication of signers and protection of integrity.

KSI blockchain: One-way collision-free hash functions are used in keyless cryptography, and keyless signature procedures include hashing, aggregation, and publication. A keyless signature allows the KSI keyless signature infrastructure to be introduced. The KSI authentication depends on the security of the hash functions and the existence of a blockchain public ledger. This ledger is public, and there are well-established laws for updating, consensus, and mode of service.

This type of blockchain was developed to solve issues related to mainstream blockchain technologies, such as scalability, time for consensus, and lack of formal evidence of security.

In a blockchain cloud, with the increasing granularity of metrics, the issue of uncertainty becomes more interesting. Better scalability is given by the non-dependence on the number of sensor measurements. However, all changes to the ledger still require fast consensus and synchronous availability.

Ericsson and *Guardtime* have adopted *the KSI blockchain technology* to their cloud computing platforms to assure data of provenance that will make real-time monitoring of cloud processes and scalable data feasible.

Putting All Together

Typically, cloud computing networks consist of numerous nodes (physical computers) running one or more virtual machines (VMs). There is an owner for each VM, and it runs program (application resources), data, etc.

When VM executes a program, and data get exchanged with the VM, multiple artifacts (variables, etc.) are produced. They are interesting pieces of information for the provenance.

Blockchain is a peer-to-peer database framework where, for straightforward authentication and auditing, interesting data for provenance can be kept online. In short, transparency and cost-effectiveness are accomplished, while access control and privacy are guaranteed by encryption strategies for cloud customers. In short, transparency and cost-effectiveness are accomplished, while access control and privacy are guaranteed by encryption strategies for cloud customers, in addition to the functionality of asset transfer which is a very important functionality of the cloud.

5.2 Blockchain Cloud Vulnerabilities

The blockchain cloud assumes that most of the network's nodes are true, trustworthy, and genuine.

The cloud environment, however, makes no promises regarding the honesty or legitimacy of its customers. Therefore, it is likely to have dishonest participants that may adversely influence the mining and/or consensus process. In the blockchain cloud environment, below is a list of bugs and attacks that can still take place.

5.2.1 Double-Spending Attack

This attack is feasible for nodes that have strong hash poser and can generate, compared to the public blockchain, the longest private chain. It is a vulnerability presented since the beginning of the blockchain with Satoshi and Bitcoin. It refers to the spending of the same digital currency for more than one transaction. The steps of this attack are the following:

1. From block N, mining to privately enlarge the blockchain as far as possible.
2. Broadcasting the exchange to the relevant organization.
3. Waiting until reasonable confirmation is obtained and the transaction is successfully registered in the blockchain such that the commodity is dispatched by the vendor.
4. Mining to expand the private branch until it is longer than that of the public branch, in secret:

If successful, advertise the hidden branch that will finally be recognized as legitimate, and discard the block containing the merchant's payment.

5.2.2 Selfish Mining Attack

The method of mining requires high computing power to solve the crypto puzzle, so pool mining refers to the union of miners with the incentive of sharing the received reward among themselves when they solve the crypto puzzle. It is helpful for the nodes to generate constant income rather than infrequent payment while mining alone.

The pool of greedy miners mine its private chain and publish it based on the state of the pool, including double-spending attacks (the length of the private chain and public one, different parent blocks). This attack technique, in short, is about the presumption that the longest chain is often acknowledged by the truthful pool. This puts the majority of trustworthy miners to join the pool, because there is no longer a space for decentralization.

5.2.3 Eclipse Attack

This attack is taking advantage of the openness and decentralization of (P2P) networks. The primary goal of this attack is to gain ownership of all a target node's incoming and outgoing communications by blocking all links from legitimate nodes.

This attack is a rapid iterative request for unsolicited connections from the managed nodes to the victim node before the victim node restarts. This raises the risk of the victim providing outgoing ties to the attacker-controlled nodes. So, the attacker becomes the only node connected to the victim, and we have a type of monopolization of all connections of the victim node. In brief, these are the steps of eclipse attack:

1. Populate the tried table by sending unsolicited messages with the IP addresses of attacker-controlled nodes.
2. Replace the current table addresses with garbage addresses (not connected to the IPs of peers).
3. When the node restarts, all the connections are monopolized with high probability.

5.2.4 Block Discarding Attack and Difficulty Raising Attack

This attack is made by a node that has a strong hold of the connections to the network. The attacker gives himself the superiority over the network by placing multiple slave nodes. So, he gets updated information about the mined blocks, and his block propagates faster than the rest of the network. So, he got the superiority to dispatch its own mined blocks and discards the blocks of others.

However, time constitutes a very important factor for this attack to succeed, due to the increase in the difficulty of the crypto puzzle that increases when the attacker's hashing power increases.

5.2.5 Block Withholding Attack [19]

In this sort of attack, the new participants of the pool contribute to reduce the pool's anticipated income. It is also known as "*sabotage*" attacks, where malicious nodes never win something, only operate against the pool, and cause them to lose the block finding game. Here, the intruder withholds the legitimate blocks and attempts to maximize his payout by sending to the pool manager as many shares as he can.

5.2.6 Anonymity Issues in Blockchain Cloud

The blockchain ecosystem is not completely anonymous for cryptocurrencies. Everyone can see the balance and transaction related to addresses in the public ledger. To track the user's identity and privacy, it must be from some information that

he can provide during a purchase or any special circumstances. So, to enhance privacy, it is better to have multiple addresses.

This feature supports darknet markets to secretly make illicit purchases. Some analysis provides a solution for de-anonymizing the transaction owner by mapping the owner's IP addresses to the addresses. Here are the moves to get the mapping done:

1. For each transaction, hypothesize an IP user.
2. Establish granular pairings of (currency address, IP).
3. For the pairings, define statistical metrics.
4. Define possible pairings that indicate genuine ownership.
5. Based on a threshold, delete unnecessary pairings.

Now that we understand the major security flaws of the implementation of the blockchain, we are going to tackle the integration of blockchain with cloud environments.

5.3 Integration of Blockchain with Cloud Environments

Cloud infrastructure is a blend of broad virtualized service networks: physical resources (CPU, disk, and network) and software resources (databases, message queuing systems, monitoring systems, load balancers).

They are referred to as "platform as a service" (PaaS), "infrastructure as a service" (IaaS), and "software as a service" (SaaS). They are hosted in massive storage centers as well.

Three key categories of cloud services can be differentiated based on resource, data storage, and associated security and privacy issues:

Public cloud: Public clouds give a diverse community of users unrestricted access to shared data and services, but there is no guarantee that the user's data will be secured.

Private cloud: Private cloud access to services and data is limited, and each account must be validated by strong protocols for authorization and authentication. Usually, private cloud clusters are operated by companies and run under a particular cloud standard.

Hybrid cloud: Hybrid clouds appear to be a perfect paradigm for the multiple private clouds to be merged into a joint global infrastructure. Via the upper-level public layer, such incorporation is achieved. The key issue with that model is finding an agreement to operate under a single public cloud standard between private cloud providers.

Therefore, a much more practical scenario is the "many cloud model" where dispersed private cloud clusters are interconnected by using the traditional P2P network. For the blockchain network, it should be remembered that a similar paradigm

operates, which was the first justification for attempting to merge these ecosystems to strengthen security policies in global clouds.

There are two key approaches for cloud integration of blockchain platforms:

1. *Usage of the cloud to build blockchain applications* and support business network integration (private clouds) to enable transactional data collection, replication, and connectivity
2. *Using blockchain techniques to enhance* task, user, and data storage security in the clouds

Both methods have their challenges, special conditions, and problems related to security. We are going to discuss them below.

5.4 Cloud Support for Blockchain Transactions and Data: Challenges and Requirements

The enormous amount of transactions generated in the blockchain network and the large volume of data exchanged expresses the need for a scalable data processing service. Meanwhile, the cloud offers a high degree of elasticity and scalability for progressing workload dynamically.

We have the public clouds that can provide a large-scale network of available services for users who pays just for what they utilize. As well, we find that private clouds do not need to be optimized to handle large datasets.

The actual location of data can be shielded by cloud systems. The continuity of the tuning activities with a low impact on the deployment of the applications represents an important equation for the effective implementation of the most blockchain algorithms.

Blockchain deployment must consider the laws of data ownership and modify data in the region allowed by the regulations. That is important to the fact that cloud services owe their owners the luxury of controlling the places where data is stored.

The use of several computing frameworks and the replication of data processed in data centers strengthens the blockchain networks' stability and fault tolerance. So, the failure of a node will not affect the work of the whole blockchain network.

The other benefit of introducing cloud blockchain algorithms is that it is possible to manage applications in a distributed cloud environment and to archive its data on a local data server (e.g., *project Oracle Blockchain Cloud Service (Oracle, 2017) and project iEx.ec (iEx.ec, 2018)*).

5.5 Blockchain Support for Cloud Users, Task, and Data Management

The blockchain is an inspiring paradigm to guarantee anonymity in the cloud environments of the user's info. The adoption of blockchain's proof-of-concept algorithms will guarantee that data and job scheduling are safe in the cloud. For example, the "model of several clouds" is an overview of the architecture of the distributed P2P cloud cluster, where the cloud service provider serves each node and the SP itself will have a complex architecture. In this case, blockchain may have a huge advantage in tracking the execution of the optimal schedule created for the list of data storage servers, cloud services, and providers of cloud resources.

5.6 The Integration of Blockchain and Cloud of Things

As discussed earlier, blockchain provides many security functions to the cloud and the cloud of things, such as integrity, transparency, and privacy, which are very helpful to fix the security challenges in the Cloud of Things. The most desirable feature of the blockchain to the Cloud of Things is the scalability capacity [20].

The Cloud of Things applies to the combination of cloud computing with the IoT. The contributions of cloud computing here are large resources, powerful computation, massive storage service, and efficient data administration, while IoT contributes to the capacity of physical instruments to track, interconnect, and diversify connectivity scenarios.

The Cloud of Things has suffered from several attacks, such as *eavesdropping, disruptive IoT attacks, unsecured means of communication, and connection quality loss*, and serious risks, *from storage and computing attacks, virtual machine (VM) migration attacks, to injection of ransomware and denial-of-service (DOS) attacks*.

There are different challenges with the Cloud of Things, like effective data storage, connectivity, and service provisions. The deployment of the Cloud of Things here is to include the need for security optimization with flexible resources.

Blockchain and Cloud of Things (BCot) represent a combination of the complementary field to overpass their limitation and disadvantages and opening up for new challenges to improve BCoT-based applications.

5.7 Motivation of Integration of Blockchain and Cloud of Things

Cloud of Things' security poses a vital challenge to its development; however, it provides massive data storage and high service efficiency. Most of the Cloud of Things computing activities come from IoT devices, taking up new challenging

security concerns such as data usability, illegal data sharing, data protection management, privacy, identity management, and access control.

(a) *Data availability*: The actual configuration of the cloud is vulnerable to single-point failures, what threatens the availability of cloud services due to the reliance on the central management and provision of cloud services. In addition, the centralization here does not provide the equal availability of IoT services to multiple users at the same time or any alternative when the servers are disrupted.
(b) *Privacy management*: The vast quantity of data stored on the dynamic cloud poses critical questions regarding the safety of consumer data. Users put their trust in the cloud, which pushes them to outsource their data protection to the cloud, which implies losing control of their data, which often has detrimental effects on data ownership.

In comparison, clustered cloud IoT paradigms with multiple clouds do not totally spread IoT files, storing them at high density in some cloud data centers. This activity leaves this volume of information vulnerable to leaks and violation of the privacy of consumers.

(c) *Identity management*: The traditional approaches for the identity management model are not suitable for the cloud IoT environment. Instead of being controlled by a central authority, it is of immense importance to have a dynamic authentication system dependent on existing user access.
(d) *Data integrity*: Data integrity in the Cloud of Things is performed using public verification schemes that call the auditor "third party" to perform a periodic verification. This process has several critical issues, such as invalid verification due to malicious auditors. Public key infrastructure (PKI) verification systems suffer from many issues, such as certificate storage, revocation, and authentication; hence, there is a need for an optimized solution for Cloud of Things applications to validate data integrity.
(e) *Access control*: The typical solutions for access control are focused on attribute-based encryption technologies that include a trusted private key generator (PKG) to configure the cloud access control policy framework. In addition to the threats of serious violence and lack of data ownership, the concern here relates to the challenge of locating a trustworthy PKG in operation.

The federated cloud networks of dispersed cloud organizations do have flaws in access control compliance that can weaken the process of access control.

Putting All Together

Figure 6 represents the large spread of the integration of blockchain within the Cloud of Things.

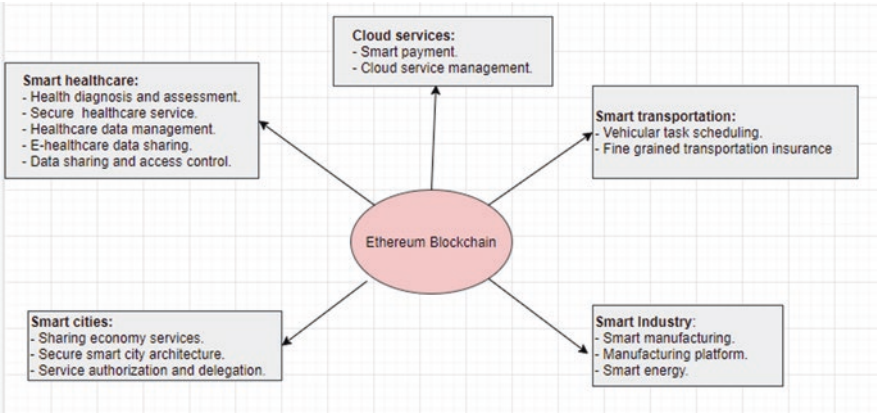


Fig. 6 Use cases of the Ethereum blockchain

5.8 Technical Limitations of Blockchain

In terms of scalability, complexity, and security weaknesses, the blockchain has many important problems:

(a) *Scalability*: The block size limitation causes a prolonged waiting period to attach transactions to the chain. In consequence, the throughput of the overall system is limited since the generation of the block is increasing. With the enormous size of the cloud, IoT data will make it very difficult for this huge blockchain size to be processed.
(b) *Complexity*: For the IoT devices have the constraints of resources which will prevent them from solving the complex mathematical puzzles that require powerful computation hardware.
(c) *Security flaw*: As we have discussed previously in this chapter, the blockchain has many security vulnerabilities that will affect its implementation on whatever system.

Putting All Together

- To have clear transaction management is the key to prevent the threats of data leaks and harm to the system.
- Blockchain may be placed at risk of data leakage and system destruction without providing robust transaction management.
- In addition to ensuring encryption and anonymity in the system, the blockchain provides the solution to all centralization problems in the Cloud of Things.
- Cloud services in the Cloud of Things improve data storage efficiency and can process intensive computations for mining.

5.9 The Opportunities for Integration of Blockchain and Cloud of Things

The corporation of such those technologies offers a wide variety of potential for BCoT:

(a) *Decentralization management*: By utilizing a peer-to-peer network of cloud nodes and IoT devices, it is feasible to create a BCot distributed management architecture. Due to decentralized consensus, all the peers have the same history of transactions, which often provides a network of no confidence problems between organizations. BCoT avoids single-point loss, prevents effective service interruption, and increases the availability of data.
(b) *Improved data privacy*: The dynamicity of data sharing between cloud services and IoT customers makes the infrastructure vulnerable to threats and data leakage triggered by adversaries or third parties. Immutability, honesty, and openness characteristics make the blockchain an appropriate data security structure in the CoT. So, for BCoT applications, the properties provided to BCoT from blockchain improve data privacy.
(c) *Improved system security*: Blockchain offers critical security properties, confidentiality, and availability. The confidentiality is ensured using the digital signature and the cryptographic hash of the recorded transactions. The replication of the recorded transaction over the participants ensures the availability of data as explained previously. In case the network is interrupted due to external threats, resourceful cloud computing can have off-chain storage options to enable data functionality with on-chain storage mechanisms. Around the same time, the stability of the blockchain system itself could be improved by this corporation. For example, for retaining and storing blockchain applications, clouds should use their available network security tools.
(d) *Improved corporation*: The combination of the blockchain and BCot systems with multi-clouds offer a secured circulation of IoT data in an untrusted environment with the management of blockchain. To prevent data breaches and maintain user privacy, the blockchain masks sensitive user information. The automated user authentication and data access offered by smart contracts help to secure data sharing in corporative BCoT.
(e) *Reduced system complexity*: The integration of blockchain with cloud computing, referred to as blockchain-as-a-service, refers to the platforms that are ready to configure and apply blockchain for BCoT projects. The cloud infrastructure is available to run blockchain algorithms, the thing that will resource costs of the usual run of the blockchain.

5.10 Blockchain as a Service (BaaS)

The blockchain as a service (BaaS) is a cloud platform where the blockchain network is deployed and hosted. The blockchain-enabled services offered by the BaaS to endorse IoT applications are the following:

- *Shared ledger*: It represents the database shared and distributed between members of BCoT (i.e., IoT users, cloud nodes, and blockchain entities). The shared ledger tracks interactions between IoT devices and the cloud, such as data exchanging or data sharing. It allows industrial networks where cloud users can monitor and validate their transactions while connecting with the blockchain cloud.
- *Consensus*: It offers consumer transaction authentication services by using consensus processes such as PoW, PoS powered by a miners' network. In enhancing blockchain consistency and maintaining high security for the system, this service is extremely important for BCoT. Interestingly, as a part of their contributions, IoT users may use their virtual cloud machines to enter the consensus process to earn rewards.
- *Shared contract*: Smart contract services are also provided by BCoT for applications.

Smart contracts are extremely valuable for developing business sense and faith in the BCoT system with their self-execution and autonomous functionality. In addition, smart contracts offer security services for authorization of user access or verification of data exchange after transfers are conducted by IoT peer nodes and helps to preserve cloud blockchain security.

Cryptography: It is the critical tool for securing data within the cloud entities and IoT devices by providing the public key. Digital signatures ensure the integrity of this data and enhance the immutability of transactions. The management storage of IoT data in this corporation is done using the hash values and periodic implementation of verification (e.g., *IPFS (InterPlanetary File System)*).

Cloud computing services: The data coming from the IoT devices are sent to cloud servers and held in blockchain storage in the cloud. There are two ways of storing IoT data, *off-chain* (in the cloud) or *on-chain* (in the blockchain). The corporation of many clouds could have a place to make use of diverse functionalities of each type. In brief, the introduction of the blockchain in the middle layer between the IoT devices and cloud infrastructure is the best way to handle cloud interactions, facilitate the delivery of services, and avoid the conflicts among the clouds.

Remarks

Public blockchain such as Ethereum with smart contracts enables the growing need for P2P IoT network and distributed cloud to prove the potential to create scalable BCoT platforms.

Many cloud systems, such as *Amazon* (Figs. 7 and 8), *Microsoft*,

Azure, or *IBM*, have merged with blockchain to offer BCoT services for companies.

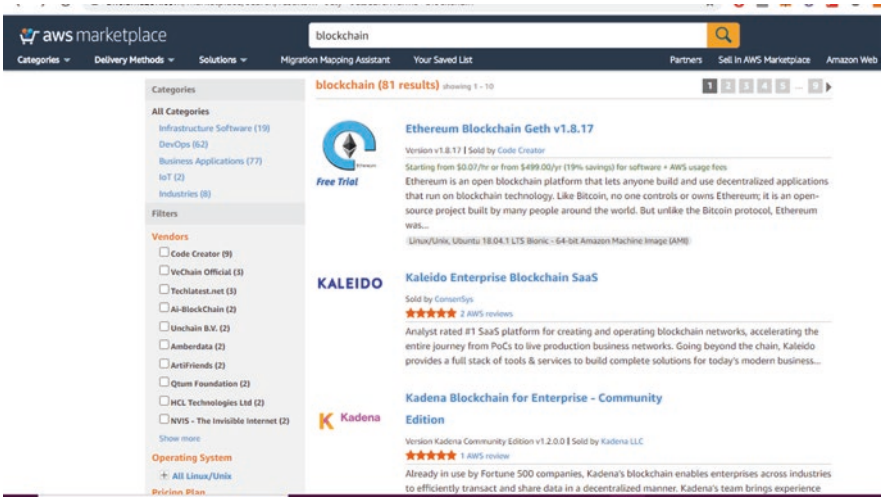


Fig. 7 The Amazon blockchain service

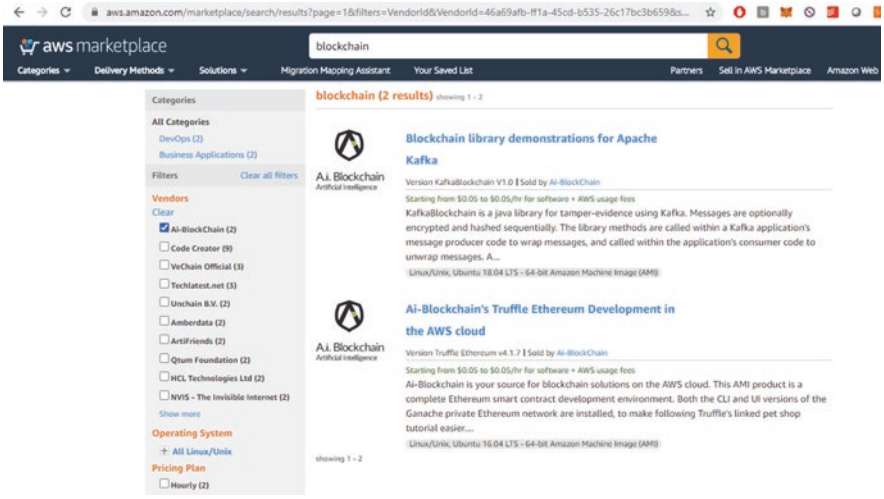


Fig. 8 Ethereum development in Aws

The growth of blockchain cloud vulnerabilities is due to the immense computational resources needed to accomplish PoW. The solution to this weakness is to follow a consensus method such as proof of stake (PoS) and perfect Byzantine fault tolerance (PBFT) that does not require high mining process computing capacity.

Putting All Together

Figure 9 introduces the different Baas platforms from 2017 to 2018. The big cloud structures are and still working on the development of the adoption of blockchain.

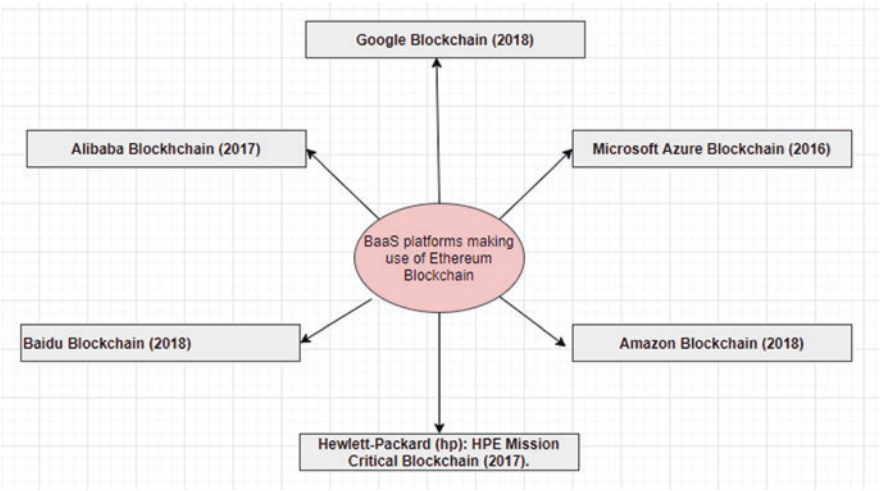


Fig. 9 BaaS platforms making use of the Ethereum blockchain

6 The Implementation of Ethereum Blockchain for Azure: Azure Workbench

As we have represented previously in this chapter, it is quite clear that the majority of the attacks on the Ethereum network is due to the feature of automaticity that it provides while making available the smart contract development to users of the network [21].

So, the first security measure that should be implemented and taken by consideration is the integrity and correctness of the smart contracts in the network, either the one in the cloud or the original environment [22].

Much research was talking about functions that can be developed with the Solidity language and make a scan to the smart contracts and exclude the ones that do not follow the security policy defined by the network users [23, 24].

6.1 Specifying the Application Policy

Workbench makes use of the smart contract to implement the security policy for the network users. It allows any customer in a JSON file to have a policy (or model) reflecting the application's high-level workflow. The policy is made up of multiple features, such as the name and description of the application, a collection of responsibilities, and a set of workflows. Each function is a collection of user addresses which provides access control or permissions for the different behavior that the application exposes.

We differentiate a global role from an example role in that the latter refers to a specific workflow case. Instance roles are supposed to often be a subset of the user addresses aligned with the global function.

Data members (or fields) have position members (requestor and responder) that range through user addresses. In addition to the constructor function, the workflow consists of two actions (or functions), *SendRequest* and *SendResponse*, each of which accept a string as an argument.

A workflow transformation consists of a starting state, an operation or a function, a collection of access controls, and a series of successor states. For example, if a user belongs to the *RESPONDER* function and invokes the *SendResponse* operation, the application may switch from *Request* to *Respond*.

An "application instance role" *(AIR)* refers to a workflow member of the example role data that stores a member of a global role (such as *Requestor*).

6.2 Implementation of Workflow

In this stage, to execute the workflow, the consumer provides a smart contract for the required blockchain ledger.

Workbench supports the common Solidity language for Ethereum targeting applications. The contract declares the data members of acceptable types present in the configuration as state variables. To track the current state of a workflow, each contract enforcing a workflow specifies an additional state variable.

The contract consists of the function of the constructor, with matching signatures, along with the two functions specified in the policy. The functions set the state variables and properly change the state variables to represent the state transitions.

Remark

- The Workbench service allows a user to upload the regulation and Solidity code and optionally connect users and execute different configuration-enabled behavior. Since the implementation is powered by the smart contract, the policy is used to expose the collection of enabled activities for a given user in each state.
- Policy and Solidity code inconsistencies can result in unintended state changes that do not agree with the high-level policy.
- It is also important to check that the Solidity software semantically conforms to the expected purpose of the policy configuration for the proper operation and protection of the application.

Putting All Together

For an application, the Workbench policy requires the user to describe:

- Data participants and an application's behavior.
- The application's high-level state machine view captures the nature of a workflow that progresses between a series of states depending on certain user behavior.

Role-based state transfer access control that provides protection for the implementation of smart contracts in a transparent and adversarial environment.

6.3 Smart Contract Security

Smart contract security techniques can be categorized as follows:

- Static techniques to identify weak structures
- Formal techniques of authentication
- Runtime checking

The static techniques: The selection of static analysis methods focused on a choice of data flow analysis or symbolic execution to identify variations of known insecure patterns that include the use of reentrancy, transaction ordering dependencies, sending ether to unconstrained addresses that can lead to the missed ether, the use of block time stamps, mishandled exceptions, calling suicide on an unconstrained address, etc. These methods only identify instances of documented patterns of vulnerability.

Formal verification techniques: It is about *checking the correctness of smart contracts*. This category focuses on the Solidity interpretation to the formal verification languages to check the translated program's correctness [25, 26].

Runtime checking: In borrowing ideas from linearizability, this method incorporates reliable reentrancy patterns at runtime.

7 Simulation of 51% Attack

To simulate the 51% attack, we need to use the *geth*. It is an implementation of the Ethereum node based on the programming language *GO*. It helps users to *mine Ether* and *run a software* in the EVM [10].

All the following steps are executed on ubuntu 14.04 with the following characteristics (Fig. 10):

Step 1: Installation of geth
We run the following commands on the terminal as a superuser Algorithm 1 (Fig. 11).

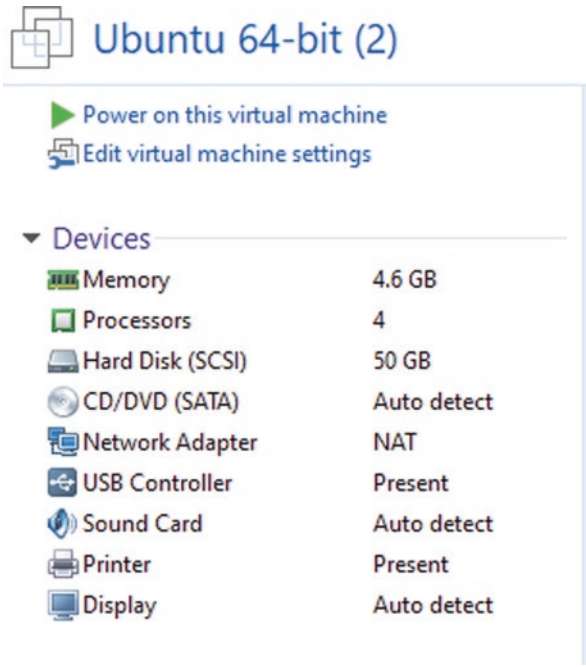


Fig. 10 The characteristics of the machine for the simulation

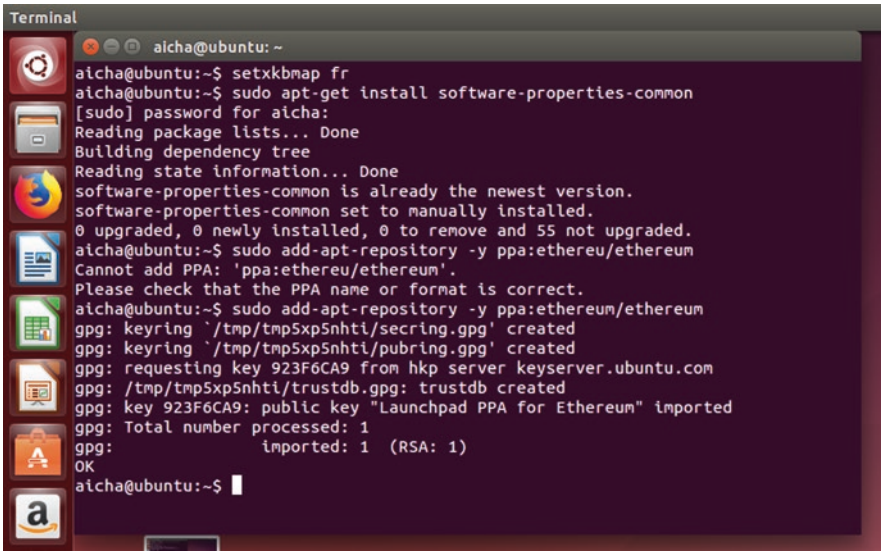


Fig. 11 Installation of the geth

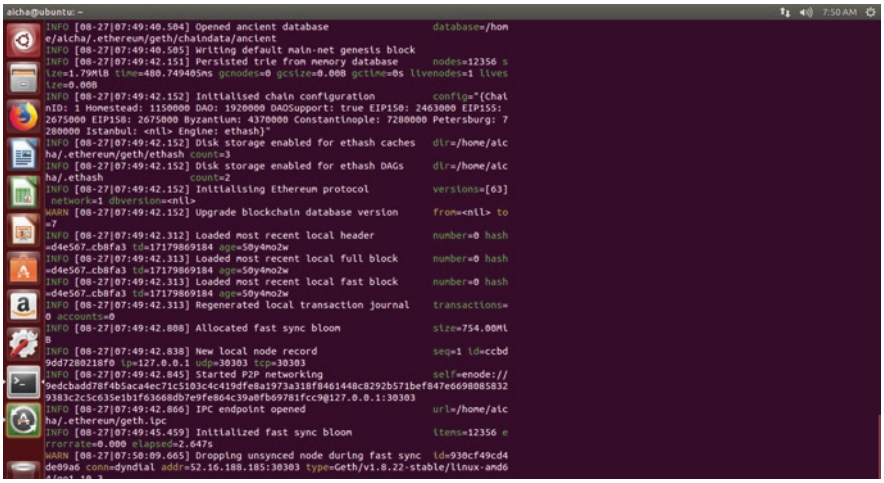


Fig. 12 Synchronization of the geth with the Ethereum blockchain

Fig. 13 genesis.json

Algorithm 1: Commands for the Installation of Geth

```
$sudo su
$apt-get install software-properties-common
$add-apt-repository -y ppa:Ethereum/Ethereum
$apt-get update
$apt-get install Ethereum
```

Launch the *geth* and let it synchronize the blockchain by executing this command (Fig. 12)**:**

```
$geth
```

For our simulation, we will need two nodes, an honest node and a malicious node, and we will need a malicious person.

Step 2: The creation of a private network
For this step, we will create a file JSON called genesis.json, which will help us create our nodes in the same network and with an initial balance Algorithm 2 (Fig. 13).

Algorithm 2: genesis.json

```
{
  "config": {
    "chainId": 666,
    "homesteadBlock": 0,
    "eip155Block": 0,
    "eip158Block": 0,
    "eip150Block": 0,
    "eip150Hash":   "0x00000000000000000000000000000000000000000000000
0000000000000000000",
    "eip155Block": 0,
    "eip158Block": 0
  },
  "gasLimit": "2100000",
  "difficulty": "1",
  "alloc": {
       "0x4e02712e277521952a568678e1863dbeb57a3ee2":{

"balance":"3000000030000300000000000000000000000000000000"
        }
    }
}
```

We will arrange it in a folder called network. Then we execute the following commands (Fig. 14):

```
$brew tap ethereum/ethereum
$ brew install ethereum
```

The following commands generate the data and keys of the accounts Algorithm 3.

Algorithm 3: The Commands for the Generation of the Data File for Accounts

```
$ geth --datadir honestMiner/data/ init network/genesis.json
$ geth --datadir maliciousMiner/data/ init network/genesis.json
$ geth - -datadir maliciousClient/data/ init network/genesis.json
```

We then create the accounts Algorithm 4 (Fig. 15).

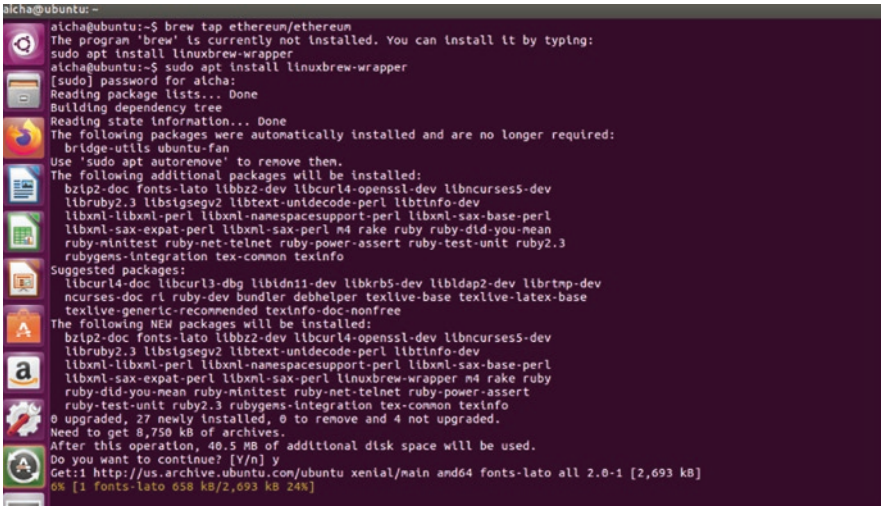


Fig. 14 Execution of the commands

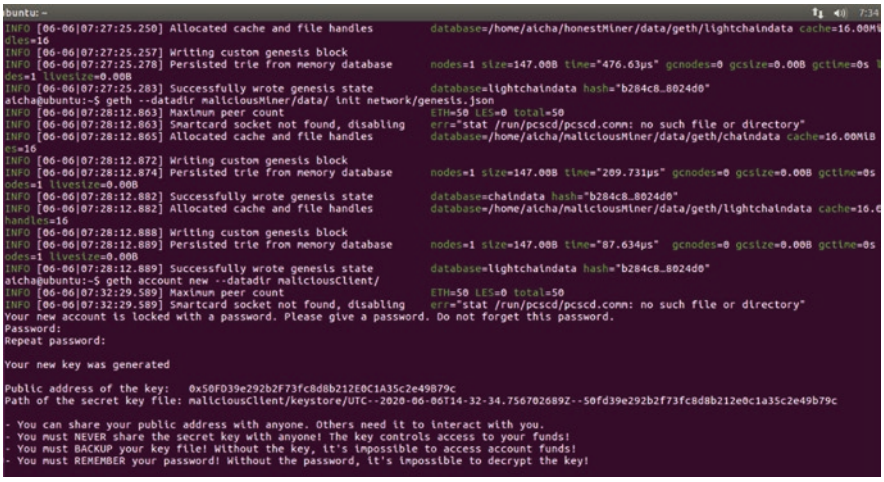


Fig. 15 The creation of the account

Algorithm 4: The Creation of the Accounts

```
$geth account new --datadir maliciousClient/
$ geth account new --datadir maliciousMiner/
$ geth account new --datadir honestMiner/
```

We remember the key and the password for each node. Now we got each account with its data file and key file.

After that, we make sure the nodes know about each other. So, we open three terminals, one for each, and we run the command:

Terminal 1:

```
$geth --datadir honestMiner/data --keystore honestMiner/keystore/
--networkid 666 --nodiscover --port 30303 console
```

Terminal 2:

```
$geth --datadir maliciousMiner/data --keystore maliciousMiner/
keystore/ --networkid 666 --nodiscover --port 30304 console
```

Terminal 3:

```
$geth --datadir maliciousClient/data --keystore maliciousClient/
keystore/ --networkid 666 --nodiscover --port 30305 console
```

We make sure every node is running on a different port of the others.

These commands take us to the JavaScript console where we are going to do all the work (Fig. 16).

Now it's time to connect the three nodes; this is done by taking the enode URL and add it to the admin.addPeer (enode URL) of the other nodes.

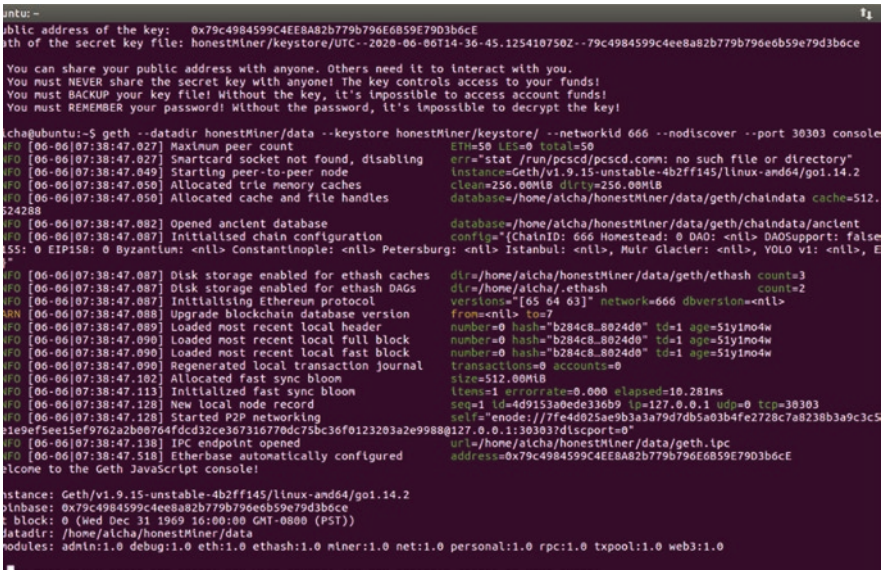


Fig. 16 JavaScript console for the honest node

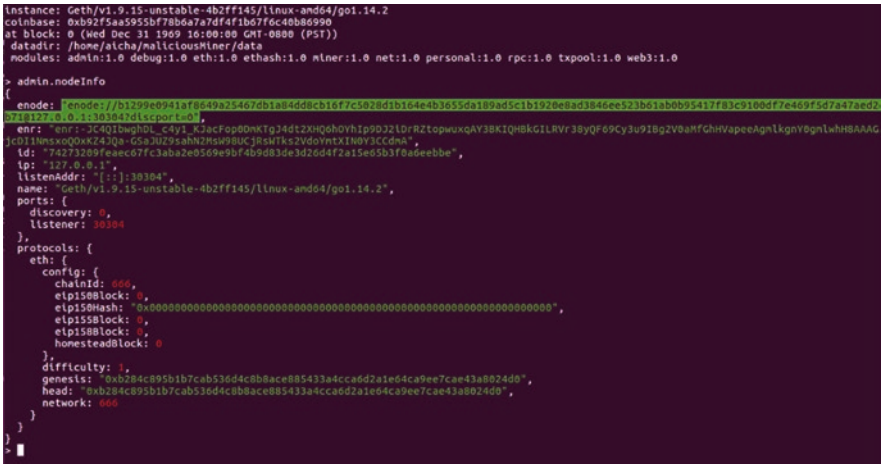


Fig. 17 The output of the admin.nodeInfo

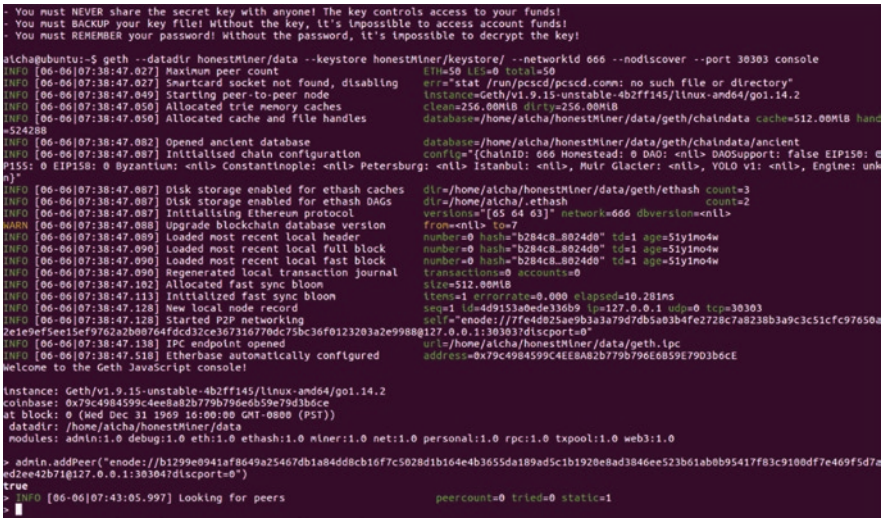


Fig. 18 The execution of admin.addPeer

We capture the enode URL of every node by running admin.nodeInfo on every terminal (Fig. 17).

We make sure that the peers are connected by running the admin.peers (Figs. 18 and 19).

We run for every terminal the command *miner.start(1)*, 1 refers to the number of threads over which the node is mining, which gives every node the same power over the network mining process and helps generate some ether for each node so we can be very sure that each node has a balance Fig. 20 (web3.eth.getBalance(eth. accounts[0]) returns the balance of the accounts)

Fig. 19 The execution of admin.peers

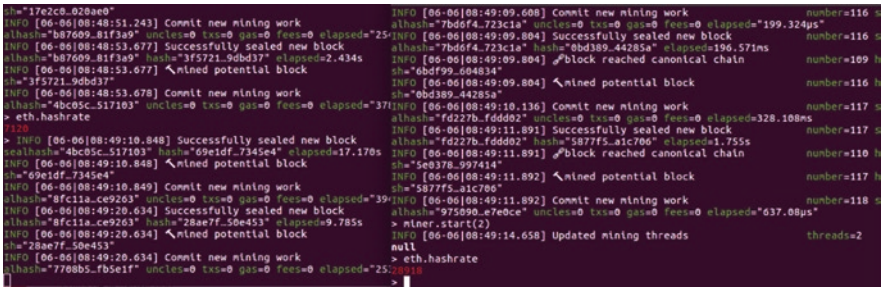


Fig. 20 The honest and malicious miners while mining

Step 3: The attack

For the 51% attack, we will run the malicious miner on a new port over two threads so to isolate it and give it time to produce a heavy chain than the one of the honest miner and stop the mining for the malicious client. We wait for the eth.hashrate of the malicious node to be superior than the eth.hashrate of the honest node. We will run a transaction that will be accepted by the honest node once the transaction is accepted by the honest miner, and we will run it again with the peering with the malicious miner. And we will verify over the honest chain if the transaction is still up [27, 28].

For our case, we have the following information, to make it easy to understand what is going on in every command.

Malicious client:

key: 0xFd5DEC92d380A4479d9074D30bfA2F9589502369.

enode:"enode://a00f5ca61bc20adb0fd2d4741befd293c3cd9f2e9fa25df797f80c-828396ca582cf6f800a5d7385114cdc0070a79b8d283c11f6762e904ec75e07fb5b20 8c5d8@127.0.0.1:30305?discport = 0"

Malicious miner:

key: 0x589f00F050c24FBe627311FACE613b53514D8641.

enode:"enode://fca2968e06e980824179782726c25562b4a2d2cf7 d52f473092f7c1a36313e221132b0b2eafa682d3bf02dda01c8ce5a11b27f1b16ce9 3d117f078a178980741@127.0.0.1:30304?discport = 0"

Honest miner:

key: 0xe0Af047b616d31Fe06EDc6491044d061914D7F35.

enode:"enode://28596b39916ddffbe1187ecdd685ecfd958edef5c22f45e8d8bf3a 76a1586d84736f6e0e7effbc6dda4e158a9597def2bfbe4f282e9700bcb3ce4ccc60ffa c49@127.0.0.1:30303?discport = 0"

Over the malicious client terminal, we will unlock the malicious account (Fig. 21):

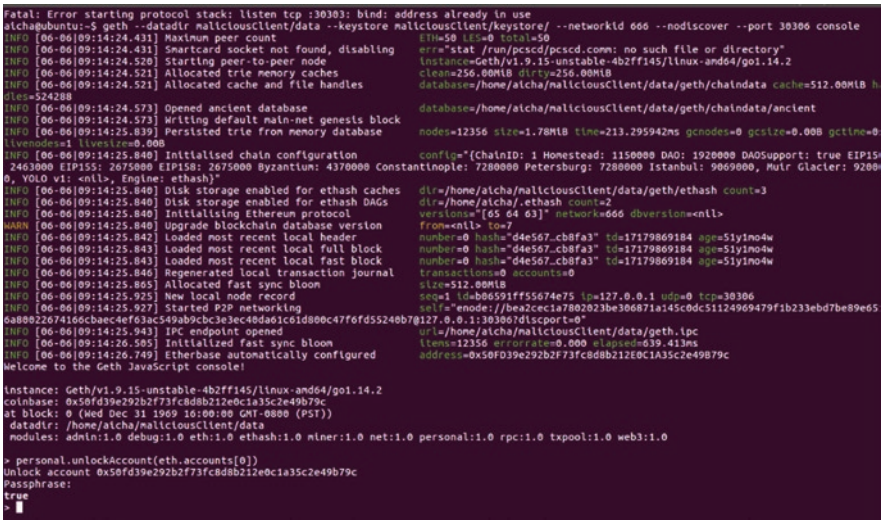


Fig. 21 Unlock of the malicious client

```
$personal.unlockAccount("0xFd5DEC92d380A4479d9074D30bfA
2F9589502369",<PASSWORD>)
```

Then we execute a transaction (Fig. 22) where the malicious client is paying the honest node:

```
$web3.eth.sendTransaction({from:   "0xFd5DEC92d380A4479d9074D30b-
fA2F9589502369", to: "0xe0Af047b616d31Fe06EDc6491044d061914D7F35",
value: 1000000000000000000})
```

The transaction execution produces the following results:

```
fullhash=0x0d2a0154206d6c12c7f67ec1a0bc7a27ecaf330662b759b1852
de650d4cb0356            recipient=0xe0Af047b616d31Fe06EDc649104
4d061914D7F35
"0x0d2a0154206d6c12c7f67ec1a0bc7a27ecaf330662b759b1852de650
d4cb0356"
```

We capture the fullhash, to use it for having access to the transaction receipt Algorithm 5 and Fig. 23:

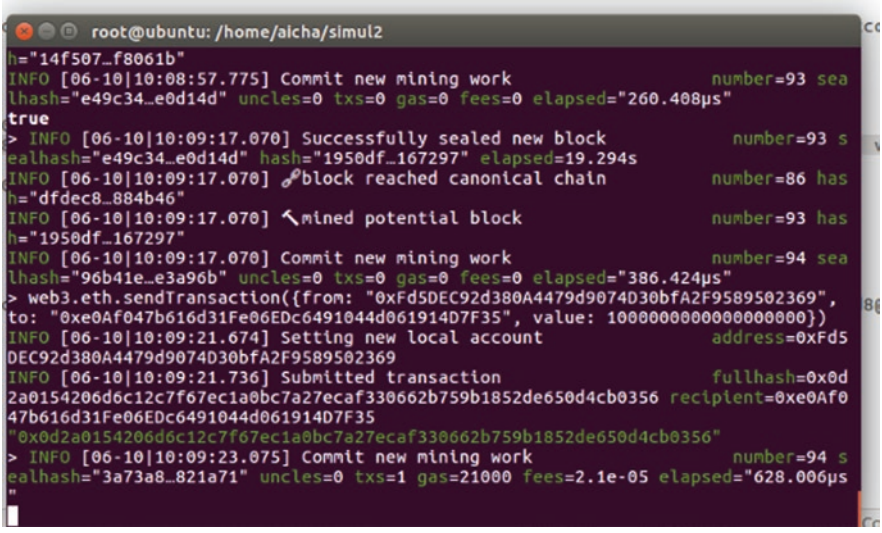


Fig. 22 The transaction

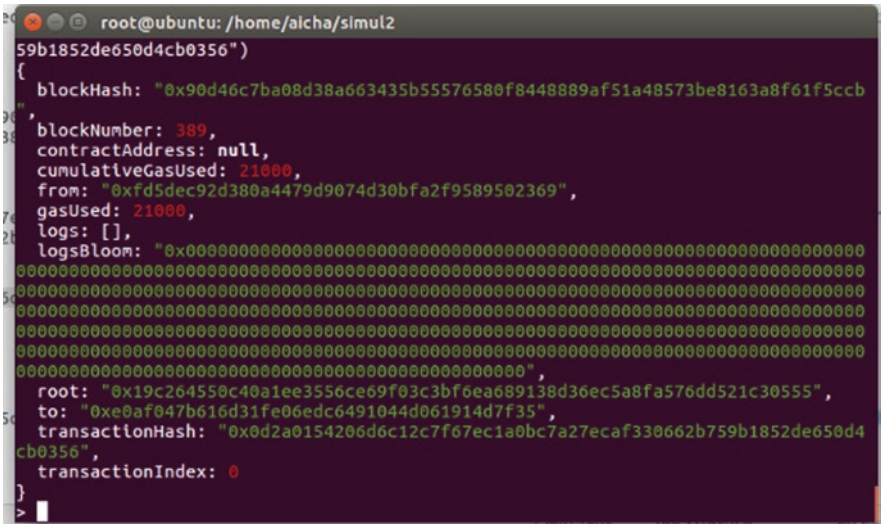


Fig. 23 Transaction receipt

```
$web3.eth.getTransactionReceipt("0x0d2a0154206d6c12c7f67ec1a0bc
7a27ecaf330662b759b1852de650d4cb0356")
```

Algorithm 5: The Transaction Receipt

```
{
                                                        blockHash:
"0x90d46c7ba08d38a663435b55576580f8448889a-
f51a48573be8163a8f61f5ccb",
  blockNumber: 389,
  contractAddress: null,
  cumulativeGasUsed: 21000,
  from: "0xfd5dec92d380a4479d9074d30bfa2f9589502369",
  gasUsed: 21000,
  logs: [],
   logsBloom:  "0x00000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000
```

```
0000000000000000000",
  root: "0x19c264550c40a1ee3556ce69f03c3bf6ea689138d36ec5a8fa576d
d521c30555",
  to: "0xe0af047b616d31fe06edc6491044d061914d7f35",
    transactionHash:  "0x0d2a0154206d6c12c7f67ec1a0bc7a27ecaf3306
62b759b1852de650d4cb0356",
  transactionIndex: 0
}
```

We then peer the malicious client with the malicious node; on the malicious client, we run the following command:

```
$admin.addPeer(enode://a00f5ca61bc20adb0fd2d4741befd293c3cd9f2e9f
a25df797f80c828396ca582cf6f800a5d7385114cdc0070a79b8d283c11f676
2e904ec75e07fb5b208c5d8@127.0.0.1:30305?discport=0")
```

eth.blockNumber returns the block number on the malicious miner (Fig. 24).

On the honest chain, we run:

```
$web3.eth.getBlock(645)
```

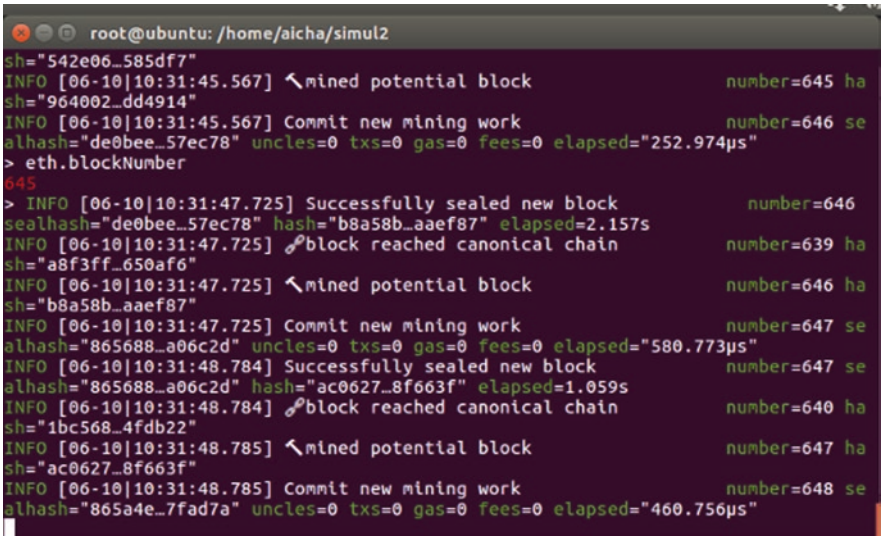


Fig. 24 The malicious node is on 645 block

Algorithm 6: Receipt of the Block in the Honest Chain


```
{
  difficulty: 174991,
  extraData: "0xd883010910846765746888676f312e31342e32856c
696e7578",
  gasLimit: 3939961,
  gasUsed: 0,
  hash: "0x9640023c9ad91c3c8a9081c13b3016b76a
6f6fb918271109fcf11f602add4914",
  logsBloom: "0x00000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000",
  miner: "0x589f00f050c24fbe627311face613b53514d8641",
  mixHash:
"0x5edfd293e155abd3c475eb27b5759614bccbbc58ba-
b075a0cf9f63ce7acdf306",
  nonce: "0x7609e57bd8398d36",
  number: 645,
  parentHash: "0x80b72ae9144879bde3c1603b5c22fd36a747103545b9f520
979fafae867c37d6",
  receiptsRoot:
"0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622f-
b5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413
f0a142fd40d49347",
  size: 538,
  stateRoot:
"0xde1b14db66097ce38164fc7f997b47606ddfd582919ee-
b6035955326a21234b2",
  timestamp: 1591810299,
  totalDifficulty: 97823352,
  transactions: [],
  transactionsRoot:
"0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622f-
b5e363b421",
  uncles: []
}
```

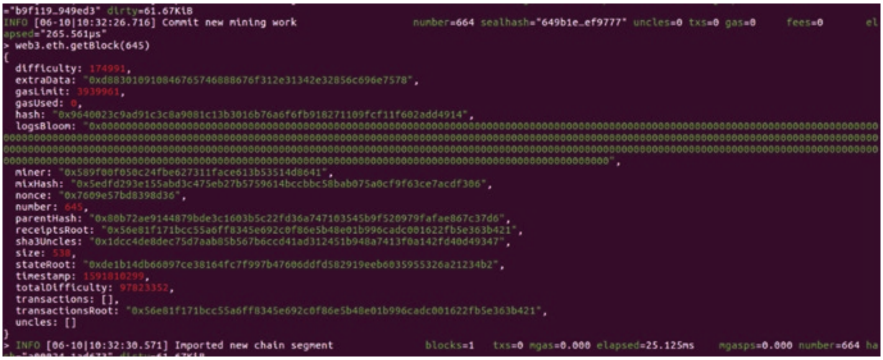


Fig. 25 The 645 block on the honest chain is empty

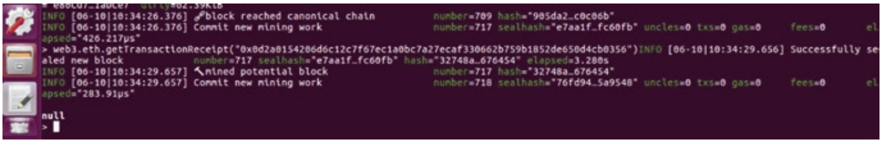


Fig. 26 No receipt for the transaction

The transactions field is empty Algorithm 6 (Fig. 25), and the receipt does not exist anymore (Fig. 26).

We found that due to the peering with the heavy chain, the malicious person succeeded to roll back the transaction, after he gained the service offered by the honest miner.

8 Conclusion

Based on the paradigm of blockchain, cryptocurrency, and game theory, and making use of its ancestors – Bitcoin – *Vitalik Buterin* builds a system that offers too many new things to the cryptocurrency field and lets the door wide open to new challenges and modifications that would work on the benefit of making the network faster and large without neglecting the importance of the security.

Security is a vital aspect to retain as the network scales, price rises, and falls draw market makers, driving much more uncertainty in moments of excessive volume of trade that drives miners to leave. Volatility provides the risk of collaboration between malicious node operators and financial market makers, pushing down the cost to decrease the hash capacity of the network and planning to fork the chain into a new state while executing a double-spend in the process.

As the Ethereum blockchain platform is one of the next-generation systems that uses a distributed ledger mechanism that is cryptographically implemented, its

security assessment is essential to ensure its utility in the cloud computing domain. Hence, we briefly addressed in this chapter the following:

- The principles of the Ethereum blockchain
- The advantages of combining the blockchain network with the elastic, flexible cloud environment to increase data server trust and data and user management security
- The problems raised by this process of integration
- Applicability and stability effects of blockchain in the application of cloud blockchain
- The bugs that could have a negative effect on the cloud infrastructure when implementing blockchain

References

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"
2. H. Chen, S. Liu, Building logistics block chain platform based on cloud computing. 2020 J. Phys.: Conf. Ser. 1486 032022
3. D.C. Nguye, P.N. Pathirana, M. Ding, A. Seneviratne, Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges
4. M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. **6**(2), 2188–2204 (2018)
5. 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. Tutor. **21**(2), 1676–1717 (2018)
6. T.M. Fernandez-Carames, P. Fraga-Lamas, A review on the use of blockchain for the internet of things. IEEE Access **6**, 32979–33001 (2018)
7. J. Park, J. Park, Blockchain security in cloud computing: Use cases, challenges, and solutions. Symmetry **9**(8), 164 (2017)
8. R.B. Uriarte, R. De Nicola, Blockchain-based decentralized cloud/fog solutions: challenges, opportunities, and standards. IEEE Commun. Standards Magazine **2**(3), 22–28 (2018)
9. R. Yang, F.R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: a survey, some research issues and challenges. IEEE Commun. Surv. Tutor. **21**(2), 1508–1532 (2019)
10. C. Dannen," Introducing Ethereum and Solidity"
11. Dr. Gavin Wood, "Ethereum: a secure decentralized generalized transaction ledger EIP-150 revision"
12. Y. Wang, S.K. Lahiri, S. Chen, R. Pan, I. Dillig, C. Born, I. Naseer, K. Ferles, Formal Verification of Workflow Policies for Smart Contracts in Azure Blockchain. *11th International Conference*, VSTTE 2019 New York City, NY, USA, July 13–14, 2019 Revised Selected Papers
13. F. Wessling, C. Ehmke, M. Hesenius, V. Gruhn, How much blockchain do you need? Towards a concept for building hybrid DApp architectures. *2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, Sweden, 2018
14. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, 2020)
15. R. Chandran, S.R. Kumar, N. Gayathri, Genetic algorithm-based tabu search for optimal energy-aware allocation of data center resources. Soft. Comput. **24**(21), 16705–16718 (2020). https://doi.org/10.1007/s00500-020-05240-9

16. V. Buterin, “Ethereum White Paper: a next generation smart contract and decentralized application platform”
17. A.B. Pedersen, M. Risius, R. Beck, “A Ten-Step Decision Path to Determine When to Use Blockchain Technologies “
18. H. Wang, H. Qin, M. Zhao, X. Wei, H. Shen, W. Susil, “Blockchain-based fair payment smart contract for public cloud storage auditing”,
19. D.K. Tosh, S. Shetty, X. Liang, C.A. Kamhoua, K.A. Kwiat, L. Njilla, “Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack”
20. D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, “Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges”
21. C. Cai, H. Duan, C. Wang, Tutorial: building secure and trustworthy blockchain applications. *2018 IEEE Cybersecurity Development (SecDev)*, USA, 2018
22. Amazon Web Services, [Online]. Available: https://aws.amazon.com/tr/blockchain/, 2019
23. Azure Blockchain, [Online]. Available: https://azure.microsoft.com/tr-tr/services/blockchain-service/, 2019
24. Y. Wang, I. Dillig, C. Born, S.K. Lahiri, S. Chen, I. Naseer, R. Pan, “Formal Specification and Verification of Smart Contracts in Azure Blockchain”
25. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
26. Sharma, S.K., Modanval, R.K., Gayathri, N., Kumar, S.R. and Ramesh, C. (2020). IMPACT OF APPLICATION OF BIG DATA ON CRYPTOCURRENCY. In Cryptocurrencies and Blockchain Technology Applications (eds G. Shrivastava, D.-N. Le and K. Sharma). https://doi.org/10.1002/9781119621201.ch10
27. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. *Blockchain, Big Data and Machine Learning: Trends and Applications*, 97 (2020)
28. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global), pp. 165–177. https://www.igi-global.com/chapter/future-blockchain-technology-for-autonomous-applicationsautonomous-vehicle/262701 https://doi.org/10.1002/9781119621201.ch010

Blockchain: Structure, Uses, and Applications in IoT

Shanu Khare, Azher Ashraf, Mir Mohammad Yousuf, and Mamoon Rashid

Abstract With the continuous increase in the applications of blockchain, the research and academic circles are constantly exploring and providing guidelines for the use of blockchain in new directions. The use of this technology has given new dimension in the Internet of Things (IoT) systems. In this chapter, the authors are providing an outline and structure of blockchain and its various applications in IoT. Blockchain technology helps in building trustless and efficient secure environment in IoT. Therefore, the authors think it is necessary to aim the basic shape of this technology and explain its use and applications in IoT in a concise and comprehensive way. This chapter starts with introduction of blockchain and IoT supported by its working in various applications of IoT. The authors believe that this chapter will provide a basic idea to users in understanding blockchain technology in IoT applications.

Keywords Blockchain · Bitcoin · IoT · Order integrity · Ownership · Transaction

1 Introduction

Blockchain was developed by Satoshi Nakamoto in 2008 as its distributed exchange registry for use in the crypto blockchain currency. Blockchain is an ever-growing list of documents, termed as blocks, which are connected and protected through cryptographic techniques [1]. Usually, each frame includes a hash algorithm message digest of cryptographic techniques, time frame, and authentication tokens from the preceding block. Blockchain is by default fundamentally immune to application of data or information alteration. It is a free public record that can effectively, verifiably, and permanently document interactions between two entities. Blockchain is primarily maintained for use as a public record by a peer-to-peer framework which adheres mutually to a consensus for confirming new blocks [2]. If registered, the data can't be modified unconstitutionally in any specific block

S. Khare · A. Ashraf · M. M. Yousuf · M. Rashid (✉)
School of Computer Science & Engineering, Lovely Professional University, Jalandhar, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_6

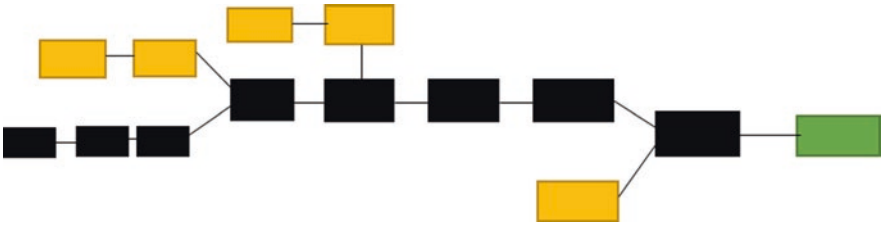


Fig. 1 Blockchain formation

without altering all corresponding blocks, which involves system network mainstream collaboration.

Blockchain is safe by nature and exemplifies a high-performance computing framework with huge appetite to medieval faults [3]. This enables blockchain theoretically ideal to store incidents, health records, and other information processing practices, such as unified communications, payment dispensation, authenticity tracking, food regulatory compliance, or polling [4]. The formation of blockchain is shown in Fig. 1. The central sequence (black) contains the maximum sequence of chains from the (green) inception frame to the present frame. Orphan frames (yellow) exist outside of the central sequence.

1.1 Blockchain Concept

Blockchain is a scattered, concerted, and communal voltaic registry that is utilized to indenture or report remittances through numerous apparatuses so that the datum or data storage cannot be subjectively altered without reforming all conforming mounts and platform involvement [5]. This supports the investors to assess remittances or payments and to assess them moderately. The blockchain platform has unconventionally functioned across a peer-to-peer groundwork and a dispersed session casting database. They are unconventionally confirmed by seeming self-interests functioned by unceasing cooperation [6]. The consequence is an unchanging procedure where there is a negligible misperception about the investor's customer statistics or information security. Blockchain utilizes eradicating the interminable methodological accuracy element from digital currency. This is assurance that each adjustable of spending has been moving only once, addressing the continuing double expenses issue. Blockchain was well-defined as an identification for the reciprocating of evaluates [7–10].

1.2 Internet of Things

The Internet of Things (IoT) is an evaluating standard that has altered the methods in our everyday livelihood and operative. The Internet of Things (IoT) is an

evaluating standard that helps different organizations to increase the value of business and help in improving decision making [11, 12]. With informal accordance among social and appliances, the rapidity of statistics or facts inception is receiving multi-fold, enlarging sharply in extent and is acquiring more aggregation. The communication of the Internet of Things is the straight unification of computer-based schemes to that of the physical world where the substances can be controlled remotely by utilizing the remaining network structure [13, 14]. With the utilization of IoT techniques, human involvement is minimalized, and this technique indicates to larger accurateness and effectiveness correspondingly. The IoT includes real-time capturing of data from sensors [15–17]. As the cost of sensors and actuators continues declining, organizations putting resources into the modern part would most likely adapt up to the cost deterrents in embracing IoT platforms [18–20].

The rest of the chapter is organized as follows: Sect. 2 discusses the history of blockchain. Working of blockchain is discussed in Sect. 3. Applications of blockchain are discussed in Sect. 4. Uses of blockchain are given in Sect. 5. Future trends of blockchain in IoT are given in Sect. 6. Finally, conclusion is given in Sect. 7.

2 History of Blockchain

Throughout the early 1980s and at the beginning of the 1990s, the key concepts underlying distributed ledger future tech came out. The paper "The Part-Time Parliament" [21] was presented by Leslie Lamport to ACM Operations on Communications Platforms in 1989; eventually, the manuscript was issued in a 1998 matter. This article identifies a paradigm of convergence for finding a settlement in a central server that cannot be accurate for the machines or system either. As an automated pioneer for the electronic authentication of agreements in 1991, a registered documentation string had been first established to readily demonstrate any absence of any of the certificates which were validated throughout the collection [21]. Table 1 shows the chronology of distributed ledger advancements.

3 Working of Blockchain

As blockchain is a collection of time stamped records that are immutable in nature and are managed by cluster of computers instead of single computer or entity. The working of blockchain contains series of steps which are shown in Fig. 2.

The working of blockchain can be summed up in terms of five steps as given below:

1. Transaction Request The core of blockchain technology is the storage of data in secure and true ways. The transaction request makes it sure that status of

Table 1 Summary of the current methodologies to the safety of published research observations

Reference	Permutations	Description
Taylor [22]	First permutation	Bitcoin, a cryptocurrency development, became an initial big blockchain exploration. Bitcoin's daily volume now stands at about $10–$20 billion, including in dozens of users including a rapid-growing content delivery sector
Böhme et al. [23]	Second permutation	Blockchain became a second development. Almost every large corporate institution in the world is actively carrying out cryptocurrency operation, and about 15 percent of businesses have expected and said that in 2017
Kosba et al. [24]	Third permutation	The third innovation was called "smart contract," something which was embodied in a decentralized system of the early 1990s, called Ltc, which specifically created techniques via IoT systems that permit transactions like government stocks or shares to be interpreted regardless of money-like Bitcoins' monies. AMD's intelligent contracts are estimated at almost 1 billion dollars and tens of thousands of businesses related to this market
Kiayias et al. [25]	Fourth permutation	The latest big development, the modern reimagining of IoT systems, is called "risk confirmation." Advanced sensing blockchains are secured by "work documentation," under which decisions are taken by the group with the highest total computing ability. Such entities are called "traders," and, in exchange for Ethereum purchases, consumers operate massive data centers to provide this security. Such energy sources are substituted by modern mechanisms, replacing structural growth mechanisms for a corresponding and better set of meanings
Eyal et al. [26]	Fifth permutation	Blockchain scaling is considered the fifth big innovation. In the cryptocurrency setting, almost any appropriate device is carried out with each transaction in the network. It's a tricky task. A decentralized blockchain aggravates the issue by computing how computers have to track each payment and then split the job efficiently, despite undermining security. That's a tough question and no obstructionist problem to handle something except compromising blockchain's respectable security or durability. The customizable blockchain should propel artificial intelligence quickly and adequately and then take on the two massive economic counterparty mediators in the world economy.

transaction between the sender and receiver is validated and completed. The Bitcoin blockchain information exists solely in relation to Bitcoin transactions under financial information. This is a huge record of success of all the financial transactions, all the way to the first Bitcoin transaction.

2. Chaining the Blocks After the transaction request data establishment, there is a connection through peer-to-peer network between nodes. This will be chaining the blocks together and connecting them to each other. In Fig. 2, there are four blocks which are chained together, and all contain the transaction data.

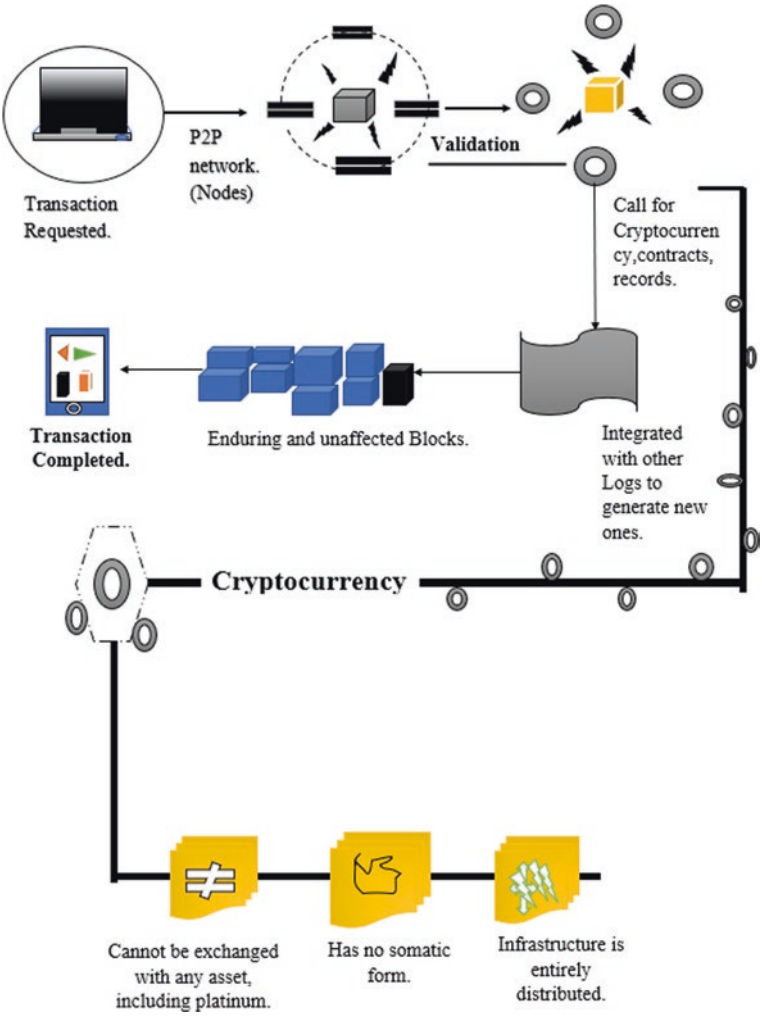


Fig. 2 Working of blockchain

3. Validation For validating, blockchain requires verification and separates the blocks from chaining. All blocks are ready for the hashing and cryptocurrency technique. Any payment has to be checked until it makes the purchase. For many other public info documents, such as the Stock Exchange Commission or the public library, there's someone in control of searching for newly document inputs. So far with blockchain, the task is given to a computer network. If they buy from Amazon, the computer system reacts to verify if your payment occurred throughout the manner you said that it would.

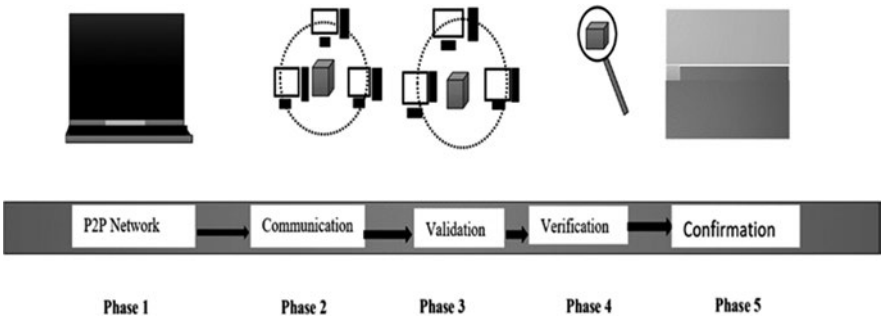


Fig. 3 Phase-wise procedure of the processes of blockchain

4. Digital Signature and Hashing In this step, all blocks call for cryptocurrency contacts record where every block needs digital signature and hashing. Hashing is a kind of way of everyone in blockchain to agree for the current world state, while digital signatures ensure that transactions are meant only for rightful owners. These are important parameters in blockchain that ensure that it will not get compromised or corrupted.

5. Integration Operations In integration, all blocks combine and attach with the logs. Upon checking the payment as correct, it receives the perfect excuse. The dollar sum of the purchase, user digital signature, and a digital signature from Amazon are mostly contained inside a file. Here, the payment is likely to contain tens to millions of such entities.

Blockchain processes contain five phases for its working as shown in Fig. 3. These phases are as follows:

Phase 1 – P2P network
Phase 2 – Communication
Phase 3 – Validation
Phase 4 – Verification
Phase 5 – Confirmation

4 Applications of Blockchain

The whole digital web is about stuff, the most precious imminent things user could access and really wants to secure. All such resources are maintained in encrypted format on a channel-to-channel string, named the blockchain or registry, whereby each individual determines with whom users are doing company. Based on these resources, there are some applications which belong to the blockchain and are given below:

- Blockchain finance
- Blockchain business
- Blockchain smart contracts
- Blockchain IoT

4.1 Blockchain Finance

Cryptocurrencies, or virtual tokens at its finest, are tokens which are transmitted across an online web. Purchases can be made through checking, transferring, or money. User could also use a kind of digital goods, perhaps commonly Bitcoin, but also Litecoin, Peercoin, or Dogecoin, and many others, in which user utilizes an electronically encrypted domain to render the payment. And more important, the payment is more secure as the user wants it to be. In order to assure confidence, conventional structures employ a negotiator, including a lender or a payment processing corporation.

4.2 Blockchain Business

Existing systems appear to be bulky, vulnerable to failure and frustratingly weak. In many cases, mediators are required to arbitrate the procedure and resolve disputes. On the other hand, customers are reporting the blockchain to be in lower cost, transparent, and more powerful. Real surprise, this device is being used by an increasing array of investment banks to implement technologies including digital securities and formal verification.

Some points of blockchain business application are as follows:

- Regulation of assets: exchange and reimbursement
- Insurance: compensation
- Handling fees: cross-border fees

4.3 Blockchain Smart Contracts

Smart contracts are electronic, implanted with such an if-this-then-that (IFTTT) software that allows them to control to operate themselves. In everyday life, an individual guarantees that conditions are met by both stakeholders. The blockchain also renounces necessity external alliance and also guarantees that certain stakeholders throughout the network know the full contingent of the agreement and therefore that implied warranties are immediately applied until the requirements are met.

Some points of application in blockchain smart contracts are as follows:

- Blockchain music
- Blockchain healthcare

4.4 Blockchain in IoT

Blockchain and IoT are crucial technologies that will have a major impact on production firms over the next few decades. These two technologies boost productivity, generate incentives for new companies, resolve legal requirements, and improve efficiency and visibility. The IoT makes it simple to analyze real-time sensor data relevant data. As the expense of detectors and sensors continues to decrease, by accepting IoT frameworks, manufacturing sectors will overcome financial barriers.

The collective use of the distributed, open, generic ledger available to investors in the organizational network would enable blockchain to share critical information gathered from the IoT.

Information security and IoT privacy are immense possible due to the vast and pervasive nature of IoT networks. For the remainder of resource-controlled IoT devices, deconcentration and security of blockchain technologies often need substantial resources, setbacks, and task processing that is not suitable.

The Internet of Things (IoT) has been sufficiently formed from its inception and is indicative of the Internet's growth in the coming time frame. One of the technical challenges is the need to handle millions of machines worldwide. While usability structures and procedures for IoT perform, they rely on structured constructs that place a fresh set of functional limitations on international administration. As the transfer moves from source to destination, the blockchain will contain relevant records from smart applications connected to products or materials.

5 Uses of Blockchain

Blockchain's predominant use currently is as a decentralized booklet for digital currencies, particularly Bitcoin. There are some areas to describe the uses of blockchain in different or various modes. These are the following:

1. General Potentials Blockchain technique has a tremendous capability to lengthy-term transformation of marketing strategies. The decentralized blockchain registry architecture is rather a fundamental innovation—capable of building a newer base for foreign socioeconomic structures. Through using blockchain, the distribution networks, electronic communications, and institutional investors and distributed instant messaging of public networking frameworks are offering major levels of efficiency.

In principle, the collection of taxes, transportation, and hazard control by blockchain will be feasible. With a centralized database, blockchain cuts payment control procedure costs, and by eliminating necessity trustworthy "external parties," such as financial organizations, to execute payments, the system also decreases connectivity expenses, supporting many submissions. Blockchain technique, which begins with a heavy focus on economic implementations, expands to practices like distributed and interactive implementations that remove an intermediary.

2. Land Registrations Structures and hearings including the one at the Sweden Companies house seek to show the blockchain's efficacy in accelerating surface selling transactions. The Republic of Georgia is channeling blockchain-constructed material goods archive. Tokens and experiments such as those carried out in the Sweden Property Register are intended to show the productivity of the blockchain in accelerating land selling agreements. Georgia is conducting the repository of blockchain properties. India's administration of government is using the blockchain to counter property corruption.

3. Smart Contracts Ledger-based intelligent transactions are transactions which, without human involvement, can be accidentally or deliberately implemented or performed. Computerized issuer is one of the key goals of an intelligent agreement. The IMF is of the opinion that the ledger can reduce perverse incentives and maximize transaction use in overall. Their legality is not obvious due to the absence of common utilization.

Several blockchain applications can allow transaction programming to be executed when certain requirements are met. Through comprehensive coding guidelines that identify and implement a transaction, blockchain digital transaction will be allowed. Digital currency strength is, for instance, a decentralized accessible-source framework developed specifically to understand this alternative through the implementation of a Fleming absolute coding language or programming language to enforce these transactions.

4. Financial Contrast The implementation of smart blockchain contracts provides management multitude of financial contracts on blockchain. Economic contracts identified as derivative products are especially suitable for implementing blockchains. This is because they are agreements which are based on appreciating value. The conduct of the appreciating value offers the critical incident which induces the execution of the agreement.

Blockchain provides group authentication which ensures that depositors involved in financial transactions are safe. It is also offering a continuous and official database of all the agreements and what occurred in them so that government regulators could use to recognize the occurrences on the sector in brief and those who have invested in accountability. Through streamlining financial products, performance can be improved, and market operational visibility for regulatory authorities and investment costs can be minimized. Many modern economic derivatives are exchanged across the board, which implies their trading is uninformative and stores organizations to collect massive fees for their role as financial intercessors.

5. Asset Tracking Another potential utilization case for blockchain is with an asset monitoring method toward proving possession or authenticity of a given asset. The involvement in the global supply chain of illegal merchandise and so-called conflict diamonds is a concern that needs to be addressed. A device of publicity must be visible, unchanged, and verified property documents which can be investigated at a certain moment in time to evaluate how a specific event is produced. Blockchain precisely gives this number of characteristics and therefore suits this rule. It will find things simpler for everybody to decide about who controls what and make runs in all exchanges surrounding every single item because it has changed ownership in the global marketplace.

6. Payment System Blockchain can be used for the implementation of payment systems in fiat currency. This is a logical outgrowth of its capacity to control cryptocurrencies' payments and transactions.

7. Digital Identity Just as blockchain is used to monitor the purchase of assets and their authenticity, it can be used to purchase people's identity. Assume that someone's citizenship is held on a blockchain and it will permit users to send documents as blockchain payments. This ensures the track of exchange within or outside countries. That ensures they're unchangeable, verified by the society, and centrally planned. By introducing payment systems to the scheme, it may also be feasible to transmit regulations to refuse access to only certain individuals besides punitive measures toward places of destination, security purposes, or indeed any purpose but to have others to enforce immediately on the blockchain. Everything should be transparent and standardized to allow mechanical failure to meet a process. The requirements should be clear.

8. Global Trade and Commerce Many corporations and consortia are encouraged to modify everyone's outdated technology because of the influence of blockchain technologies on global trade finance services. The impactful effect of Ethereum blockchain is recognized in the operation of global supply chains by massive trading businesses around the world, the management of financial transactions, and the opening of new business models. Further, from the time of digitalization, the framework allows current records, bank guarantees, and further digital signatures.

9. Real Estate Real estate makes use of blockchain to activate electronic real estate possibilities. The job with ConsenSys develops new business opportunities, improves the underlying property operational activities, reduces prices, eliminates information silos, and improves the market.

10. Capital Market In a time of higher results, the innovation of the blockchain changed the capital market technique to understand trade. In modern times, there have been tough restrictions, institutions, and obligations in the share market architectural style. The associated risk involves high administrative expenses and prompts industry by undermining the financial position and potential customers by raising the degree of entry. The methodology of blockchain can enhance operating expenses downwards through the available, implemented, unavoidable, and growing factual sources between such banks and financial institutions.

11. Copyright or Intellectual Property and Royalty Protection Intellectual property and ownership rules on music and other information have become increasingly vague in a world with increasing internet access. Blockchain would greatly enhance these intellectual property rules to make that the artist or originator of the material acquired is given a decent share of the electronic content uploads. The blockchain will also provide artists and content producers with full detail and accurate copyright allocation information.

12. Digital Voting Blockchain allows the capability to vote digitally, even though regulatory authorities should be able and see if something has changed in the channel. It mixes the accessibility of digital voting with the blockchain's indivisibility (i.e., the unchangeable scientific community) to categorize the voting rights of all.

13. Immutable Data Backup Blockchain could be an excellent way to retrieve information. While cloud services storage programs are implemented to become a go-to origin for information security, they are not resistant to attackers or even issues with architecture. Utilizing blockchain as a backup device for the cloud computing environment or any information could address this problem through GPS receivers itself on routes.

14. Medical Record-Keeping The excellent thing is that for years now the health industry is already shifting away from document for documentation purpose. Yet blockchain offers that much greater safety and efficiency. To get medical information, it will be in charge of the medical information, who has the right to obtain these electronic records and has exposure of handling these documents. It would be a matter to enhance the HIPAA rules that secure patient confidentiality.

15. Data Sharing In November, Cryptocurrency IOTA released a beta version of all its primary data sources, illustrating that blockchain could be used as a consumer market to exchange or exchange discarded information. Because most company information passes unclaimed, blockchain can serve as an interface to purchase and migrate this information to achieve a series of businesses. While in its initial stages, IOTA has far more than 35 brand name members (one of them being Microsoft) providing feedback.

6 Future Trends of Blockchain in IoT

Apache blockchain is generally used for maintaining conformity with laws, boosting inventory monitoring and enhancing identity security, only to mention a few instances. Blockchain performs differently with several conventional centralized networks and holds log files of all activities indefinitely. In addition, several small firms, businesses, state agencies, and individuals can also use this platform. In several industries and confidence, this combination of blockchain with IoT can establish greater accountability and deter manipulation as most of the industries prosper and adopt this innovation. A collection of why the human race adopts the whole innovation and the adjustments we can see is presented below:

Higher Consumer Acceptance We might see a massive requirement for IoT in the next 20 years when everyone needs anonymity, protection, and above all time-saving capability. Blockchain is needed to boost this IoT requirement and to function reliably. Therefore, as consumption rises, production growth improves, and businesses embrace the modern ideology of technological breakthroughs. The IoT infrastructure will be built, and travel, protection, and farming problems will dramatically decrease.

Market Rise in Home Automation Everyone needs luxury, and it can be done by intelligent houses. Think you get home on a warm weather afternoon and would like to have your AC unit on and space pretty chilly, what if you just hit and press the button on your smartphone? Such trends are going on and might grow rapidly. Presently blockchain can do it by clicking on the button by transmitting and receiving the information for both you and your air conditioner; it appears natural, but we don't really want full access, and we never want to exploit or exchange our information. That's the area in which blockchain steps in, and we will monitor the operation, i.e., who did it if it happens. This is a prime demonstration and is always challenging to protect information at excessive densities.

Need in Public Well-Being Services Followed by the community services, this innovation will grow significantly. It's still been assessed all around the global economy. There are a range of monitoring technologies, and the customer's full surgical records and photographs and pre-diagnostic symptoms may be saved in the database. Their daily well-being could be registered, and they might be utilized across situations.

Distributed Ledger Incorporation and Advanced Analytics IoT In the near future, when the future IOT models in their functionality start to be implemented by various industries, AI is in force. Typically businesses such as Sentrian, Manna, Veros Networks, Neura, etc. use IoT AI and will eventually implement blockchain, and the applications will be much improved. Blockchain owns and operates on regular machines, and an immense quantity of energy is necessary to perform the job. And both of this can be combined with a great deal of time and storage, and slowly growing as technology is the key challenge here. However, if this innovation flourishes correctly, analysis issues, AI coding, protection, and several others may be generated.

Blockchain Organizations on IoT As competition for blockchain specialists and, in particular, for citizens with awareness of IoT is growing, it is also essential. Since separate schools aim to solve both, still a distance remains, and we sense as we learners are interested in different industries. That's why various companies have their own systems where they freshen up their talents to get their industry ready, but this entire phase is too grueling for the business, and they'll continue to pay the costs.

Electricity and Capital Control Blockchain and IoT Regulation In order to handle the money we have and the electricity properly, use of IoT equipment with blockchain technologies would become an important commodity. In our houses and workplaces, to hold the humidity, sprayers, etc., we can have IoT gadgets. Active

identification and efficient utilization of energy, remote identification, and elevated usage power, thanks to the blockchain embedded with IoT, we may render all of these visible information. This will enable us to deter and track climate change, the conservation of soils, protected areas and all the community industry MNC, etc., concerns that have little impact on our climate.

Augmentation of IOT Appliances with Blockchain 95% of businesses with their service equipment would be IoT. As per Gartner, the corporations are now considering increasing the extension of these. It is important to make the products increasingly robust and to enable anyone to use and prosper from this.

7 Conclusion

In this chapter, the authors provided an outline and structure of blockchain and its various applications in IoT. As blockchain technology helps in building trustless and efficient secure environment in IoT, the authors discussed this technology in this chapter and explained its use and applications in IoT in a concise and comprehensive way. The use of this technology has given new dimension in the Internet of Things systems. Moreover, the future trends of blockchain technology in IoT are included in this chapter. The authors believe that this chapter will provide a basic idea to users in understanding blockchain technology in IoT applications.

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. R. Matzutt, J. Hiller, M. Henze, J.H. Ziegeldorf, D. Müllmann, O. Hohlfeld, K. Wehrle, A quantitative analysis of the impact of arbitrary blockchain content on bitcoin, in *International Conference on Financial Cryptography and Data Security*, (Springer, Berlin, Heidelberg, 2018, February), pp. 420–438
3. E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.K. Fedorov, Quantum-secured blockchain. Quantum Sci. Technol. **3**(3), 035004 (2018)
4. P. Tasatanattakool, C. Techapanupreeda, Blockchain: Challenges and applications, in *2018 International Conference on Information Networking (ICOIN)*, (IEEE, 2018, January), pp. 473–475
5. P. Gomber, O. Hinz, M. Nofer, D. Schiereck, Blockchain. Bus. Inf. Syst. Eng. Springer **59**(3), 183–187 (2017)
6. A. Bahga, V.K. Madisetti, Blockchain platform for industrial internet of things. J. Softw. Eng. Appl. **9**(10), 533–546 (2016)
7. S. Pongnumkul, C. Siripanpornchana, S. Thajchayapong, Performance analysis of private blockchain platforms in varying workloads, in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, (IEEE, 2017, July), pp. 1–6
8. A. Banotra, J.S. Sharma, S. Gupta, S.K. Gupta, M. Rashid, Use of blockchain and Internet of Things for securing data in healthcare systems, in *Multimedia Security*, (Springer, Singapore, 2021), pp. 255–267

9. A. Banotra, S. Gupta, S.K. Gupta, M. Rashid, Asset security in data of Internet of Things using blockchain technology, in *Multimedia Security*, (Springer, Singapore, 2021), pp. 269–281
10. F. Syed, S.K. Gupta, S. Hamood Alsamhi, M. Rashid, X. Liu, A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans. Emerg. Telecommun. Technol., e4133 (2020)
11. P.P. Ray, A survey on Internet of Things architectures. J. King Saud Univ. Comput. Inf. Sci. **30**(3), 291–319 (2018)
12. M. Rashid, I. Nazeer, S.K. Gupta, Z. Khanam, Internet of Things: Architecture, challenges, and future directions, in *Emerging Trends and Impacts of the Internet of Things in Libraries*, (IGI Global, Hershey, 2020), pp. 87–104
13. P. Singh, E. Rashid, Smart home automation deployment on third party cloud using Internet of Things. J. Bioinf. Intell. Control **4**(1), 31–34 (2015)
14. H.N. Dai, Z. Zheng, Y. Zhang, Blockchain for Internet of Things: A survey. IEEE Internet Things J. **6**(5), 8076–8094 (2019)
15. M. Rashid, S.A. Parah, A.R. Wani, S.K. Gupta, Securing E-health IoT data on cloud systems using novel extended role based access control model, in *Internet of Things (IoT)*, (Springer, Cham, 2020), pp. 473–489
16. E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions. IEEE Trans. Ind. Inf. **14**(11), 4724–4734 (2018)
17. P. Sethi, S.R. Sarangi, Internet of things: Architectures, protocols, and applications. J. Elect. Comput. Eng. **2017**, 1–25 (2017)
18. M. Rashid, H. Singh, V. Goyal, N. Ahmad, N. Mogla, Efficient big data-based storage and processing model in Internet of Things for improving accuracy fault detection in industrial processes, in *Security and Privacy Issues in Sensor Networks and IoT*, (IGI Global, Hershey, 2020), pp. 215–230
19. D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: A top-down survey. Comput. Netw. **141**, 199–221 (2018)
20. S. Al-Sarawi, M. Anbar, K. Alieyan, M. Alzubaidi, Internet of Things (IoT) communication protocols, in *2017 8th International conference on information technology (ICIT)*, (IEEE, 2017, May), pp. 685–690
21. G. Ateniese, B. Magri, D. Venturi, E. Andrade, Redactable blockchain–or–rewriting history in bitcoin and friends, in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, (IEEE, 2017, April), pp. 111–126
22. M.B. Taylor, Bitcoin and the age of bespoke silicon, in *2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*, (IEEE, 2013, September), pp. 1–10
23. R. Böhme, N. Christin, B. Edelman, T. Moore, Bitcoin: Economics, technology, and governance. J. Econ. Perspect. **29**(2), 213–238 (2015)
24. A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in *2016 IEEE Symposium on Security and Privacy (SP)*, (IEEE, 2016, May), pp. 839–858
25. A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in *Annual International Cryptology Conference*, (Springer, Cham, 2017, August), pp. 357–388
26. I. Eyal, A.E. Gencer, E.G. Sirer, R. Van Renesse, Bitcoin-ng: A scalable blockchain protocol, in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, (2016), pp. 45–59

Securing IoT Communications Using Blockchain Technology

Shweta Sharma

Abstract The Internet of Things (IoT) is logically an actuality today. Eventually, particular key moves despite everything ought to be given explicit thought so that IoT courses of action further assist creating enthusiasm for related contraptions and the organizations publicized. Due to the conceivable relevance and affectability of organizations, IoT courses of action should address the security and assurance concerns enveloping these devices and the data they assemble and make and the procedure. Starting late, blockchain advancement has expanded a great deal of thought in IoT courses of action. Its fundamental use circumstances are in the budgetary space, where blockchain makes an encouraging request worldwide and can be used to understand security and assurance issues. In any case, this rising development has an unfathomable potential in the most different mechanical domains and would altogether be able to help achieve the Internet of Things see in different points of view, extending the restriction of decentralization, empowering interchanges, enabling new trade models, and allowing self-administering coordination of the devices.

Keywords Internet of things · Blockchain technology · Blockchain-based internet of things · Secure IoT communication using blockchain · Communication model · Blockchain model

1 Introduction

A quick developing arrangement of innovations that help the change of business and mission forms. The IoT has arrived at different degrees of development across segments, for example, shopper, transportation, vitality, medicinal services, manufacturing, retail, and money-related. The IoT is among the framework organization of physical gadgets, for example, associated vehicles, savvy structures, mechanical control frameworks, automaton, and apply autonomy frameworks, and various

S. Sharma (✉)
MDSU Ajmer, Ajmer, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_7

things introduced with equipment, programming, sensors, actuators, and framework organize that engage these articles to exchange data [1, 2].

IoT and blockchain are two innovations that are picking up notoriety since the hour of their creation. Sooner rather than later, IoT is going to impact pretty much consistently things we use today. As the use of this innovation builds, the danger to abuse it likewise increments. Existing innovations are insufficient to manage this. Thus, blockchain has risen as a powerful answer for comprehending the security issues identified with IoT.

Blockchain Technology

Blockchain modernization is presently appropriating a great agreement of thought. It can reform and restructure the wide-reaching foundation of the advances connected along with one another through the Internet. The two fields that will be influenced by it are as follows:

- It makes a distributed background and evacuates the uncomfortable preference of central workers and provides spread association.
- This creates eventual upfront and undeveloped to all database, which carries truthfulness to the management and choices.

This technology has four elements:

1. *Consensus*: Provides the evidence of work (EOW) and approves the movement in the structures.
2. *Ledger*: Provides the total subtleties of exchange inside systems.
3. *Cryptography*: Makes sure that completely material in record and structures get mixed and simply endorsed customer can interpret the information.
4. *Smart Contracts*: It is utilized to confirm and approve the members of the system.

2 The Internet of Things

IoT suggests an around coupled plan of various heterogeneous and homogeneous devices that can identify, method, and framework. The Internet of Things (IoT) is an organic arrangement of ever-growing multifaceted nature; it's the accompanying surge of improvement that will refine everything in our life, and it is the accompanying level of motorization for each article we use. IoT is conveying a consistently expanding number of things into the mechanized cover every day, which will most likely make IoT a multi-trillion dollar industry shortly [3–5]. To find out the size of excitement for the snare of things (IoT) check what number of social affairs, articles, and studies drove about IoT starting late, this interest has hit fever contribute point 2016 a similar number of associations see enormous possibility and acknowledge that IoT holds the assurance to expand and improve associations shapes and revive advancement. In any case, the quick headway of the IoT publicize has caused an impact in the number and grouping of IoT game plans, which made certifiable challenges as the business propels, generally, the desperate necessity for an ensured

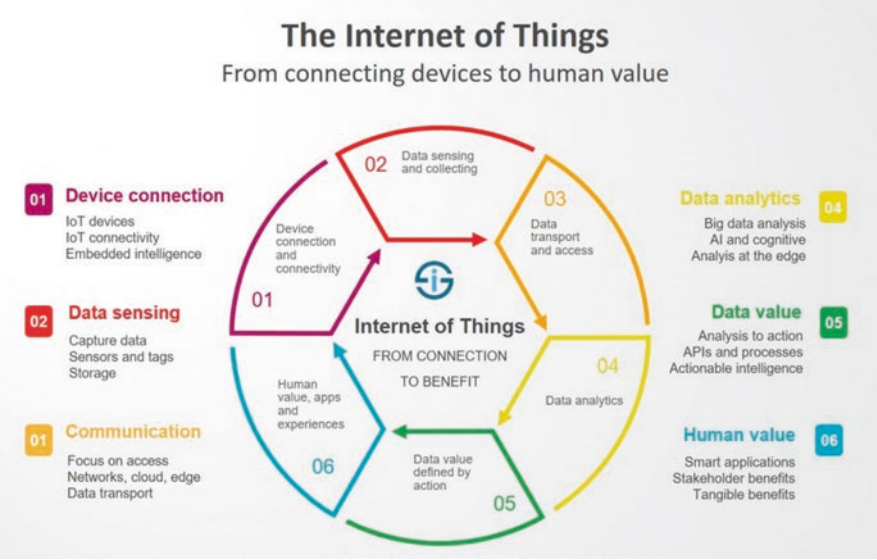


Fig. 1 IoT

IoT model to perform ordinary tasks, for instance, identifying, getting ready, accumulating, and granting. Working up that model will never be a basic task in any capacity whatsoever; various snags and troubles are going up against a certified secure IoT model. There are various viewpoints on IoT, from "system see" which isolated IoT into squares explicitly (things, gateways, network services, and cloud services) to "business see" of IoT (platform, connectivity, business model, and applications). Despite how we depict IoT, there is one rehashing subject among all points of view which is "security is principal" (Fig. 1).

Web of Things (IoT) considers the production of systems of modern brilliant gadgets, for example, telephones, keen vehicles, and shrewd home apparatuses. The expected advantages of such systems are beyond any reasonable amount to list here, yet models incorporate everything from permitting homes to gain proficiency with their tenant's standards of conduct so they can progressively mechanize errands, for example, reordering food and so on, to permitting shrewd vehicles to be prepared and holding up outside your entryway to head to you to work toward the beginning of the day.

In all actuality, these models may be somewhat way off, yet effectively a gigantic scope of savvy gadgets is accessible to shoppers. There are approximately 9 billion savvy gadgets of some kind online today. This figure is set to ascend to around 30 billion by 2020, which will compare to just about three brilliant gadgets for every individual on the planet.

A key segment of IoT is information. To work, an IoT arrangement must send and get a lot of touchy information. One such model is that the security gets the information that is required for the August Smart Lock. This savvy lock permits mortgage holders to open their home just by utilizing their telephone, without the requirement for a key.

Normally, property holders should be guaranteed that no unapproved individual will be ready to take section code information and access their home. This implies the IoT arrangement must be secure consistently. Not just that, information is regularly moved between gadgets that have various overseers and information utilization arrangements, in this way making a difficult administration condition that additionally requires close consideration regarding information security.

As indicated by an article distributed in eSecurity Planet, 48 percent of US organizations using IoT have suffered security breaches. This is a stunning figure, especially when we consider this incorporates probably the greatest and most secure organization system on the planet. The figure stresses the requirement for another way to deal with information security.

The IoT incorporates the handling of information and the correspondence between gadgets of various stages and limits of autonomic, deprived of human intercession. In ongoing times, this term design is a development of the web and introduced themselves as another innovative and common worldview. The Internet of Things is viewed as an augmentation of the existing web, and it gives registering and correspondence to interface items to the web. The association with the overall PC system will empower the controller of articles and permit the items to be gotten to as administrations suppliers, making them shrewd items.

As of now, there is anything but a solitary meaning of IoT. Be that as it may, a few creators and foundations have added to the development of his vision. IoT as an assortment of things or items, for example, labels for the radio recurrence (RFID) recognizable proof, sensors, actuators, and mobile phones. These gadgets interface with one another helping out its neighbors to accomplishing shared objectives. The creator isolates these dreams toward web-arranged (middleware), thing situated sensors and actuators, and semantics-arranged (the portrayal and data stockpiling).

Various pertinent establishments take accentuated idea that the IoT must concentrate primarily on "things," and the route to its complete execution must start with the expansion in the effects insight. A few definitions in the writing got after this vision, one of them a proposition by the exploration bunch in the IoT (European research cluster on the Internet of Things (IERC)).

3 Blockchain

Blockchain's thought begins to explain that it goes far past the mechanical turn of events. It is having an imperative impact, essentially by moving the business course halfway to a decentralized structure, introducing constancy on deceitful pros trades, without the necessity for a widely appealing substance trusted by both. Besides, the situation can convert the method of understanding fully exchange categories and empower an extensive scope of potential outcomes in different regions, for example, multi-party computation (MPC), use in decentralized autonomous organizations (DAO), and government applications [6, 7].

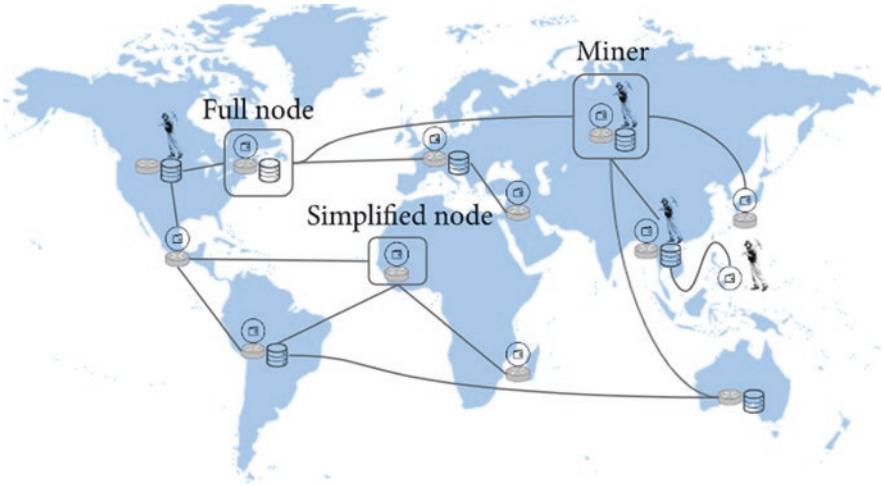


Fig. 2 Bitcoin network

A blockchain administration, or a "blockchain," is an exchange storehouse where exchanges are assembled into squares. "Each square covers a hash of the past square. This has the effect of creating a chain of squares from the earliest starting point straight to the current square." The substance of every square is carefully marked to guarantee the information honesty of recorded exchanges.

Definition Blockchain as a part to ensure suitability, constant nature, and nonrepudiation to offer sanctuary to electronic trades, filling in as a goliath coursed record. This instrument is the basic progression introduced by Bitcoin. It speaks to an approach to agree with temperamental members. As a rule, establishments like banks or public accountant workplaces are liable for the guardianship and security of the exchange record; they are called confided in outsiders. The framework proposed by Nakamoto dispenses with the need of these substances, since all the libraries are, other than open, kept up in a decentralized path by a few members of the system. Figure 2 is a system disentangled view, where we can watch the primary capacities that every hub can utilize. The situation is an intersection arrange. An intersection arrange is a system that is based on the head of another system, making layers of system reflection giving new applications or safety benefits.

3.1 Segments of a Blockchain

Blockchain mostly has four parts:

1. *A network of nodes*: All the hubs associated through the web keep up all the exchanges made on a blockchain arrange cooperatively, and the credibility of exchange is checked by a convention. At the point when another exchange

happens, its records are added to the record of past exchange which is known as "mining." Different hubs present on the system confirm the verification of work. Free hubs self-rulingly create and register real exchanges into the conveyed record. Neither a focal authority nor a believed outsider is important to approve exchanges. All hubs of the blockchain administration (additionally called the blockchain stage) team up to keep up a consistency of the record. Every hub runs a modified component called an agreement [8]. The accord is the procedure by which hubs concede how to refresh the blockchain because of a lot of exchanges. Accomplishing accord guarantees most of the hubs in the system have approved a similar arrangement of exchanges.

2. *Distributed database system*: The database is made out of squares of data and is duplicated to each hub of the framework. Each square has a rundown of exchanges, a timestamp, and the data which connects to the past square. The objective of the appropriated accord is to keep the records of an adequate lion's share of the framework peers address and forward-thinking (at a generally granular time scale). A record is worked after some time as new exchanges are included, and it is accessible and repeated across hubs in the framework (along these lines "circulated record"). Each hub on the system has its duplicate of the database and can get to the historical backdrop of any. The blockchain size of specific cryptographic money will drive prerequisites for capacity limit inside IoT and different gadgets that have the record.
3. *Consensus*: Accord components guard against vindictive companions that can degenerate the trustworthiness of the record by (a) retroactively altering exchanges; (b) performing semantically unpermitted exchanges (e.g., "double-spending" and moving not-possessed resources in a digital currency setting); or (c) hindering the acknowledgment and booking of right exchange requests. The agreement approach picked during the improvement of the blockchain administration makes preparations for explicit assaults. These assault alleviations are not simply specialized in nature. With Bitcoin's "Evidence of Work," for instance, there is a financial disincentive to overseeing 51 percent of the hash power inside the system. Increasing 51 percent of the mining hash rate would possibly permit an assailant to twofold spend coins or modify an ongoing history of exchanges. Additionally, increasing 51 percent of the hash rate and proliferating pernicious exchanges would quickly decimate trust in the digital currency and altogether decline the estimation of the noxious party's stake. What's more, that noxious gathering could just utilize their hash power toward the way toward digging to create gains for themselves.
4. *Smart contract*: Smart agreements are a self-executing code living on a record. Utilizing keen agreements, two gatherings direct an exchange. For instance, one gathering can deliver help, while the other party gives installment to that administration. Savvy contracts authorize the guidelines of the exchange and can likewise implement punishments related to resistance. With regard to the IoT, gadgets can be preconfigured to connect with keen agreements dependent on the agreement addresses on the blockchain. These gadgets would then be able to go into exchanges between one another. The keen agreement screens the progression

of the exchange and approves that rules have been followed before delivering reserves or permitting an activity. Implementers of IoT frameworks that utilize keen agreements must consider potential abuse cases and introduce rules inside the agreements themselves. For instance, a savvy contract designer may uphold escrow prerequisites that hold assets until confirmation of the shrewd agreement terms of finish. Other security contemplations when working with shrewd agreements incorporate the need to maintain a strategic distance from race situations, whereby the arrangement might be implemented all over again preceding the primary agreement exchange being finished, approving that the sender and recipient of the agreement are not utilizing a similar location and guaranteeing that lone-approved gadgets utilize the brilliant agreements.

5. Shared record: The record is made openly accessible and is ethical which is refreshed each time an exchange is made.
6. Cryptography: Data is limited by a cryptosystem which makes it difficult for unapproved clients to access or alter it.

3.2 Actualizing a Blockchain

Three spaces in which blockchain can be sent:

- *Public*: Bitcoin and Ethereum go under this class. Every single hub can send or peruse exchange without requiring any authorization. The agreement is available to the general society.
- *Consortium region*: It goes under halfway authorization. The consent to peruse or send might be made open or might be given distinctly to not many approved hubs.
- *Private*: Only the association to whom the system of blockchain has a place can compose exchange to it.

4 Blockchain-Based Internet of Things

Example of IoT dependent on blockchain:

A Communication Model
The three major elements of blockchain arrange are in this model:

1. *Peer-to-peer informing*
2. *Distributed information sharing*
3. *Autonomous coordination with the gadget*

Impediments
- *Slow Processing*
- *Small Storage*

In this model, blockchain centers are the people from the framework. They can be computers, adventure laborers, or moreover cloud-based center points. Clients are the IoT contraptions. Blockchain clients and center points speak with each other through APIs. Clients make trades, and these trades are moved to center points for dealing with and taking care of the data into the scattered document.

Interfacing various blockchain systems
In the future, diverse blockchains may fill various needs. The blockchain system might be a home system, venture, or the web. If computerized reasoning is added to the IoT condition that is associated with a blockchain arrange, it makes a decentralize autonomous association that runs without human intercession.

5 Secure IoT Communication Using Blockchain

- Blockchain is a decentralized framework that can help take care of the issues of versatility, dependability, and protection in the IoT, and it can help process exchanges. Blockchain engineers can build the security of IoT systems utilizing blockchain innovation.
- Blockchain innovation improves the security and execution of the IoT organization by giving information unchanging nature, decentralization, and keen agreements. Blockchain's protected and perpetual stockpiling empowers engineers to move code safely to IoT gadgets. Blockchain additionally makes sure about the correspondence between IoT gadgets by putting away information in exchanges and approving exchanges between hubs.
- The decentralized nature of the blockchain framework takes out assaults from a solitary point and will add to the security of conveyed information, for example, brilliant agreements, information stockpiling, and information transmission.
- Cooperation can occur in a mixture design that incorporates both the IoT organization and the blockchain. Given that blockchain is equipped for tackling significant security issues in IoT systems, it has developed a key innovation for the eventual fate of the IoT, which relies upon making a system of various gadgets that can be associated with the Internet and the cloud. Blockchain adopts a decentralized strategy that improves trust and straightforwardness between IoT gadgets, guarantees the following of associated gadgets, and manufactures a completely tough framework that is more averse to succumb to cybersecurity assaults.
- This innovation could upset IoT organizes by including another layer of cloud to the registering of IoT gadgets. This methodology includes utilizing blockchain to store just a piece of the IoT information; however, it is viewed as one of the most secure because it permits gadgets to work disconnected.

- Blockchain's distributed geography gives a protected domain to brilliant agreements and the other rationale and relics on which edge-trade exchanges depend. Related to a dispersed IoT cloud, blockchain can forestall exchanges in any event, when individual edge passage hubs are not, at this point, accessible. With appropriated blockchains and IoT systems, astute agreement specialists introduced on every hub can execute exchanges continuously, giving an extra degree of strength and protection against digital assaults.
- Blockchain-based cybersecurity arrangements can likewise utilize the software-defined perimeter (SDP) engineering and the zero trust model to make validated gadgets imperceptible to aggressors. Each new gadget added to the system is enrolled with a one of a kind computerized ID related to a blockchain organize. All correspondence between checked endorsers and IoT gadgets is cryptographically secure and put away in carefully designed conventions. The stage gives secure access to every single associated gadget and gives a protected, cross-stage correspondence arrangement.
- This implies that lone checked gadgets can perceive the presence of other associated gadgets and realize what includes an extra layer of security to the IoT framework.
- By adding cryptography to savvy gadgets, we can guarantee secure information transmission and capacity. With this methodology, the blockchain can keep up a perpetual history of smart gadget correspondence over the IoT organization. Blockchain additionally guarantees confided invalidation and approval of keen devices, implying that all information on the IoT organization is made sure about.
- To register a client's personality, most blockchain stages utilize a decentralized methodology that requires a key generator on the blockchain to make a private and open key pair. The private key stays with the client just and is utilized to demonstrate personality, while open keys are disseminated to arrange suppliers.
- Blockchain origination can be applied to follow billions of connected gadgets and allow exchange treatment and organization among them. It gives critical investment funds to IoT enterprises and producers and is a missing connection that tends to huge numbers of the security and protection issues in the IoT business. It can make a stronger biological system for working machines, just as lower costs for makers and customers.
- Blockchain's decentralized texture additionally empowers the sending of keen agreements and shrewd agreement specialists on the edge of an IoT to arrange, quickening exchanges at the edges of the texture.
- IoT gadgets are relied upon to back off—easing back down, blockchain systems can deal with this without hindering exchange speed or information stream.
- Blockchain and IoT innovations are continually advancing, taking care of existing issues, and experiencing new ones. This combination implies that designers should consider the requirement for security, protection, and information security, just as interoperability between IoT gadgets and blockchain.

6 Approaches to Strengthen IoT Security Through Blockchain Technology

For a safe utilization of the Internet of Things, the accompanying focuses are to be thought of:

1. *Secure Communication*
   IoT device need to give to exchange data required to method a trade and collect it in a record. Accounts can moreover be used to store encryption keys to make the exchanges more of a mystery. IoT device sends an encoded message using the open key of the objective contraption, which is then taken care of in the blockchain sort out. The sender by then demands that its center gets the open key of the beneficiary from the record. By then, the sender scrambles the message using the open key of the recipient; thus, simply the gatherer will have the alternative to decrypt the sent message using their secretive key.
2. *Authentication of Clients*
   The contributor carefully symbols communication before sending them to different devices. The getting gadget at that point gets the open key from the record and uses it to confirm the computerized mark of the got message. The advanced mark work is portrayed underneath:

   - Sender computes a hash of communication that is then scrambled with its secretive key.
   - The computerized sign together with the statement is sent.
   - The beneficiary at that point translates the advanced mark applying the exposed key of contributor put absent in the record to obtain the hash an incentive as resolute through the sender.
   - The message is substantial just if the resolute hash and the confirmed hash of the communication are similar.
   - The conviction on improved messages is developed if the computerized spot of all communication is placed away within the record.

3. *Finding Credible IOT Wherever Scale*
   While another IoT device instigates, it requests rootworkers to provide a rundown of confided in hubs in the structure. This device by then registers itself in a center point, and the exchanging of information starts. DNSSec must be executed to make sure about the name goal of rootworkers by staying away from any satirizing assaults. Each correspondence caused must be verified and encoded effectively. This should be possibly dependent on the following:

   - Credentials as of now introduced on the gadget during the arrangement.
   - Credentials could be given by the owner of the IoT contraption.

4. *Positioning IoT*
   Blockchain innovation assists a countless compact in setting up a confidential and protected enterprise for IoT gadgets. Approaches that appear to be important here are as follows:

Properties of IoT like configuration nuances and the last structure firmware affirmed can be encouraged on the record. During bootstrap, the blockchain center point is drawn nearer to get its structure from the record. The plan is required to be mixed in the record to hinder the revelation of IoT arranges geology or its properties by examination of the information set aside in the open record.

The hash estimation of the latest structure record for every device can be encouraged in the record. Using a cloud organization, the IoT device ought to transfer the latest and accepted arrangement record after each fixed time span. By then, the device can use the blockchain center point API to recoup and arrange the hash regard, which is taken care of in the blockchain. This would permit the managers to evacuate any terrible arrangements normally and reboot every single IoT gadget in the system with the most recent and confided in setups.

Making sure about the system of IoT gadgets through a blockchain organize types the framework distributed, in which there is no particular position that can endorse several exchanges. Every single gadget will have a duplicate of the consistently developing chain of information. This implies at whatever point somebody wishes to get to the gadget and do some exchange; at that point, all the individuals from the system must approve it. Subsequently, the approval is finished, the accomplished exchange is put away in a square and is referred to all the hubs of the system. This makes the framework safer and unimaginable for the unapproved bases to break toward safety.

7 How a Blockchain Works

Blockchain can drastically increment both the security and level of computerization of specific information exchanges. The innovation takes into consideration the production of individual squares of information as a chain. As each new square is added to the last, it structures what is, fundamentally, an advanced record containing all the data at any point added to the blockchain (Fig. 3).

Since the information on each new square is mostly determined from data hung on the past square in the blockchain, to modify a square, an unapproved individual would need to change the data on all the squares connected to it to keep the change from being promptly taken note. On account of a cryptographic money blockchain, for instance, this may well mean changing every square on the chain.

The truly energizing thing about blockchain innovation is that it works as a shared decentralized system. As such a system, blockchains don't require any controlling gathering to work. This has tremendous ramifications for huge numbers of the business forms we as a whole depend on today.

More than some other model, Bitcoin has demonstrated that it is conceivable to make blockchain-based arrangements that permit us to circumnavigate incredible establishments, which as of not long ago have had a restraining infrastructure on these procedures.

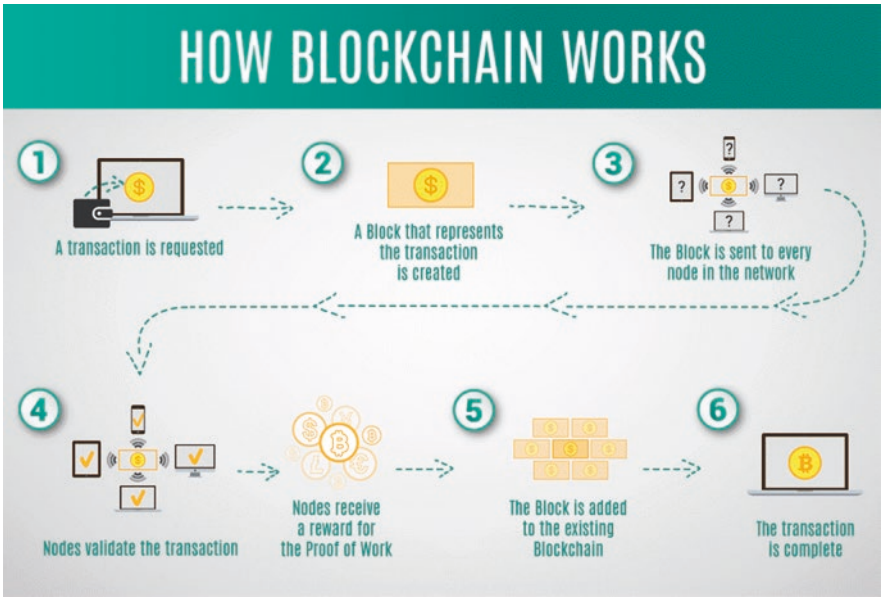


Fig. 3 Blockchain works

Another key factor in this decentralized methodology is that all the companions or "hubs" engaged with the system must concur on whatever changes are to be made. So should a programmer or other unapproved party endeavor to roll out an improvement to the computerized record without consent, different hubs will oppose this change and keep the information from being adjusted.

The principal way somebody would be able to modify the blockchain is to oversee most of the hubs on the system simultaneously to effectively finish the change. While considering how troublesome this would be, simply remember that every hub has its own novel access key code too.

Just to give you a thought of the monstrosity of the assignment, as of May 2016, Ethereum's system had 25,000 dynamic hubs implying that any endeavor to modify information along these lines would be close to inconceivable.

Key Characteristics of Blockchain

- *Decentralized* – No controlling force or purpose of disappointment.
- *Immutable* – Ledgers can't be modified without the system consenting to it.
- *Facilitates trustless exchanges* – Unalterable record implies exchanges can be made to obscure gatherings with the base of hazard.
- *Distributed preparing power* – Decentralized nature implies the system shares the heap.

Favorable circumstances of blockchain

- Increased trust
- Removes the requirement for a controlling force
- Better security
- Completely records all things considered

8 How to Secure IoT with Blockchain: The Problem of Centralization

Secure IoT gadgets utilizing blockchain

IoT works as an appropriate customer/worker model that requires a manager to deal with the system. This concentrated authority is the powerless moment that it comes to IoT cybersecurity. To work typically, IoT gadgets depend on this position to decide how they act.

If there is a penetration of security at the focal position, at that point, the data being sent by the keen gadgets is to a great extent helpless before the programmers. This makes assaulting the focal power engaging digital programmers as a lot of information can be gathered in one go. A progression of digital assaults happened in 2017, a significant number of which abused this shortcoming and permitted programmers to grab touchy information identifying with a hundred of a large number of American residents.

Since the decentralized idea of blockchain innovation would invalidate any focal assault, programmers would need to target singular hubs on the system to attempt to get the information they need. In a blockchain organize, savvy gadgets can effectively take an interest in approving exchanges.

This implies the system would have the option to make preparations for any hack by approving foreordained "adequate" conduct for any abnormalities. When a gadget on the system was recognized as not acting accurately, it could be disconnected to keep it from being utilized to get to facilitate touchy information or being utilized to open an individual's home and so forth.

Make a reliable IoT condition

Blockchain records expect clients to enter a remarkable key code to get to the system. This implies all the connections/exchanges have responsibility inherent.

Any progressions made must be marked and in this manner can be followed back to whoever made them. Any unapproved changes will be forestalled by the system as none of the different hubs appended to the system will acknowledge the change.

So with regard to the graceful chain industry, for instance, shrewd gadgets could be utilized to follow things for the whole length of the flexible chain. Since things would be marked for at each progression of the chain, keeping tabs on their development should be possible progressively as well. Any absent or postponed conveyances could be followed like a flash. This would improve both the productivity and unwavering quality of any flexible chain blockchain innovation was applied to.

One such organization to understand the huge benefit of incorporating blockchain into its flexible chain the executives is Taiwanese organization OwlTing. You can peruse more about their task to utilize blockchain innovation to build sanitation here.

In the open space, such a blockchain-based IoT framework could, for instance, be utilized in schools or colleges to guarantee students were in class on the proper occasions and in any event, ensuring they were getting their work done as well. Since the guardians could likewise be remembered for the school blockchain, they

would likewise have the option to see their kids' advancement employing an approved shrewd application.

The capacity of instructors to leave input and report any bad behaviors would enable guardians by permitting them to spur/reward their youngsters on an ongoing premise. This sort of framework could likewise at long last sign the finish of those bleak parent nighttimes that understudies, guardians, and educators the same all despise going to.

9 The Communication Model

The correspondence model portrays the foundation of blockchain programming really on IoT centers just as in the cloud with application programming interfaces (APIs) to the IoT centers. The figure underneath shows a run of the mill and recognized model construction blockchain advancement and IoT when the IoT edge contraptions have solid limits that make them prepared for encouraging the trade center programming, taking care of the record, and keeping up comparability over the arrangement of the center (Fig. 4).

IoT transaction nodes
Each IoT contraption has the record and is good for looking into blockchain trades, including mining. All device is provisioned with a private key or consolidates handiness to inside self-make a private key to look into composing trades. This end-state model gives three significant limits that can be engaged with a blockchain organization.

An arrangement of self-overseeing IoT devices, together with independent coordination (for instance accord and shared educating):

- A record of exchanges where any IoT gadget can make an exchange running cryptographic highlights
- A conveyed database where any IoT gadget has a state-of-the-art adaptation of the record

Hardware requirements make accepting this model hard for IoT at present. Troubles include the following:

1. *Low getting ready*: Computations in a blockchain organization require high CPU, memory, and power limits. The noteworthy potential gear pigs in a blockchain stage are burrowing for POW; sharp understanding execution; and cryptographic rough execution.
2. *Little storing*: The volume of trades added to the record creates and gets stumbling to keep up even with little trade data.
3. *Constrained accessibility*: An IoT device may use low information move limit Internet or radio access, which can introduce execution issues during copy and coordinating through the record.

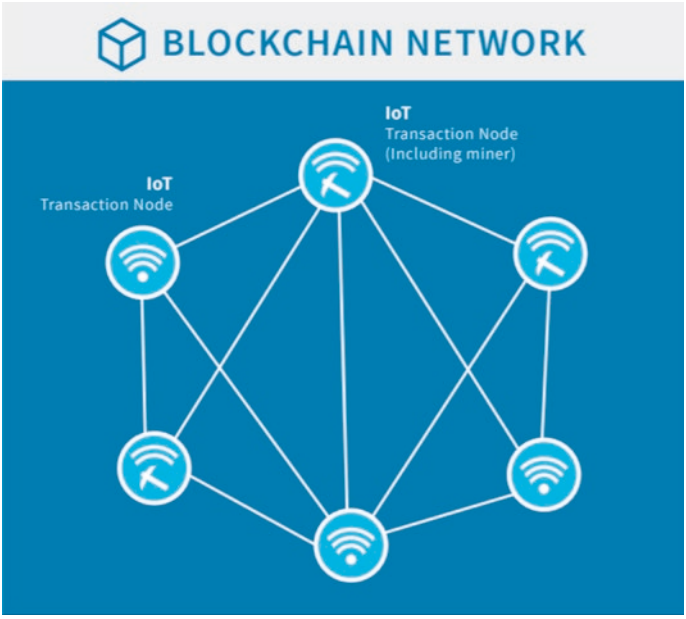


Fig. 4 Each IoT node acts as a blockchain transaction node

Cloud-Enabled IoT Blockchain Network

In a cloud-enabled blockchain framework, trade and mining centers are discovered together in the cloud and on premise. Dependent upon the execution, the centers may be attempt laborers; undertaking or personal computers or shrewd contraptions (for instance, phones or tablets); cloud-based virtual machines; and IoT devices with sufficient hardware resources (RAM and CPU accumulating, etc.) (Fig. 5).

The Internet of Things devices with limited hardware resources go about as blockchain clients. They do not stock the scattered document. The particular clients interface with upstream cloud-based blockchain trade center points by APIs. APIs will presumably be either HTTP, REST or JSON, RPC.

The Internet of Things contraptions assemble data moved to trade center points for taking care of by the blockchain backing or look into adroit agreement trades by featuring the blockchain center points running in the cloud. In this one-of-a-kind circumstance, IoT contraptions are still provisioned with private keys to sign their data. The stamped data are then sent upstream to the trade centers for taking care of. An alternate comprehension of trust between the IoT device and the trade center point must be set up to securely send data. For example, a reasonable relationship may use whitelisting and two-course confirmation between two devices (an IoT contraption and a trade center point). Hardware security should similarly be used to securely store private stamping keys.

For a permission zone (private blockchain administration), access to mining hubs might be confined to approved administrators. In a consortium zone (halfway

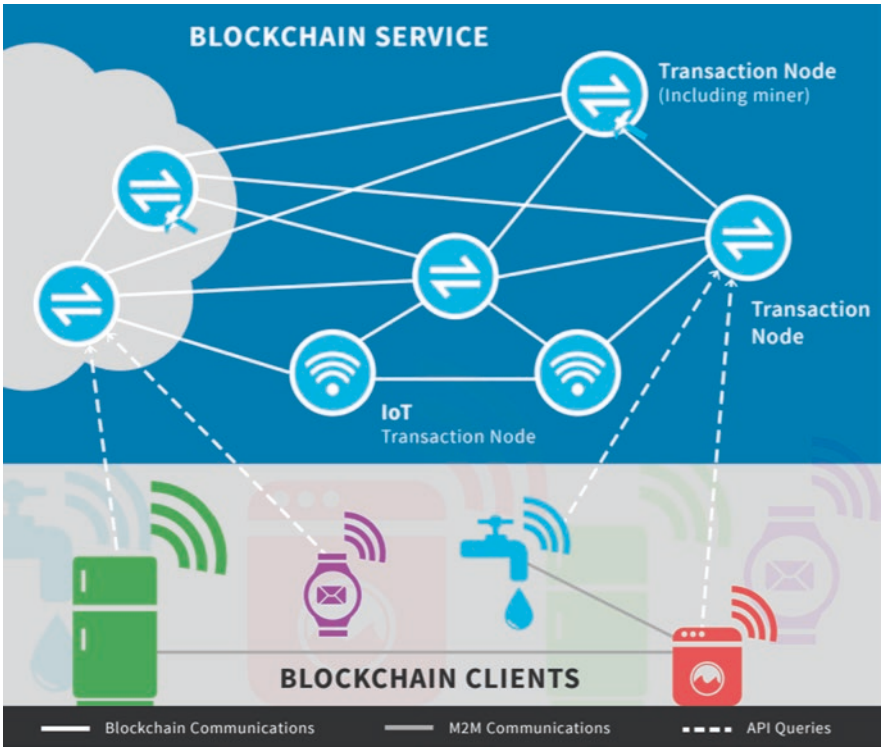


Fig. 5 Secure the IoT of utilizing the blockchain technology

permissioned blockchain administration) or a permissioned zone (private blockchain administration), individuals can choose to actualize this engineering design for improving security or for guideline consistency purposes.

Bitcoin usage proposes this sort of highlight utilizing "slight customers," additionally named simplified payment verification (SPV), which doesn't store a total duplicate of each square of the record. These "slender customers" speak with a hub utilizing Bitcoin Client API (BCCAPI).

Messages can be traded between different IoT gadgets. These messages contain information that is incorporated into the exchanges handed off by IoT gadgets partaking in the trades to the exchange hubs. Correspondence conventions and message designs between IoT gadgets are outside the extent of the blockchain usage: these interchanges allude to machine-to-machine interchanges, for example, message Queuing telemetry transport (MQTT).

10 Challenges of a Secured IOT Model

The best test going up against IoT security is beginning from the very structure of the current IoT organic framework; it's completely established on a joined model known as the laborer/client model. All devices are recognized, approved, and related

through cloud laborers that help huge taking care of and boundary limits. The relationship between contraptions should encounter the cloud, whether or not they happen to be a few feet isolated. While this model has related figuring contraptions for a significant period and will continue supporting today's IoT frameworks, it won't have the alternative to respond to the growing needs of the enormous IoT natural frameworks of tomorrow.

Cost is another large hindrance, particularly for the utilization of such a unified model in scaling up existing IoT arrangements. There is a high structure and bolster cost related to concentrated fogs, the immense specialist develops and arranging equipment. The sheer proportion of correspondences that ought to be dealt with when IoT contraptions create a huge number will assemble those costs altogether. Whether or not the wonderful money related and gathering challenges are endured, each square of the IoT configuration will remain as a bottleneck and reason for dissatisfaction that can agitate the entire framework.

There are various issues with the current brought together IoT model are; constrained heading everlastingly cycle support and the leading body of Internet of Things devices, furthermore, IoT security involvement is marvelous and not for each situation quickly obvious. Furthermore, the vocations of IoT development are developing and changing—now and again in obscure waters. Current preservation advances will be required to shield IoT contraptions and stages from physical adjusting additionally and to address new troubles, for instance, copying "things" or refusal of rest attacks that channel batteries for example. Another troublesome issue standing up to the improvement of IoT new security progressions is the way that many "things" use clear processors and working structures that may not reinforce complex security moves close.

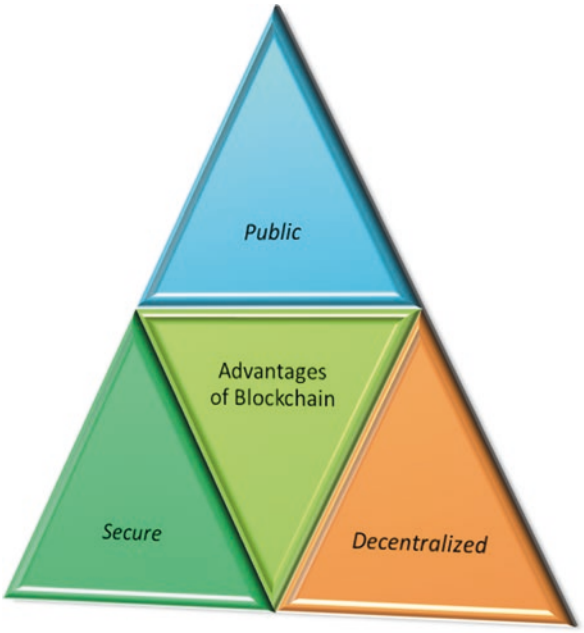
10.1 The Blockchain Model

Blockchain is a file that preserves up a reliably creating game plan of data records. It is passed on in nature, inferring that there is no pro personal computer holding the entire chain. Or on the other hand, possibly, the sharing center points have a copy of the chain. It's furthermore ever-creating—data records are simply added to the chain.

Exactly when someone needs to add a trade to the chain, all the individuals in the framework will favor it. They do this throughput on a computation to the trade to check its authenticity. What accurately is appreciated "generous" is described by the blockchain system and can differentiate between structures. By then, it is up to a lot of the individuals to agree that the trade is genuine.

A great deal of assorted trades is then bundled in a square, which gets sent to all the centers in the framework. They, in this way, endorse the new square. Every dynamic square contains a hash which is a novel interesting imprint, of the past square (Fig. 6).

Fig. 6 Blockchain model



The enormous great situation of blockchain is open. Everyone taking an intrigue can see the squares and the trades set aside in them. This doesn't mean everyone can see the genuine element of your trade, in any case; that is made sure by your secretive key.

A blockchain is decentralized; hence, presently there is no single position that can support the trades or set express guidelines to have trades recognized. That suggests there's a gigantic proportion of trust necessary later; all the individuals in the framework need to show an understanding to recognize trades.

Most importantly, it's sheltered. The database requirement is extended and records can't be changed (at any rate, there's an amazingly critical cost if someone wants to alter past document).

10.2 Benefits of Blockchain in IOT

Numerous specialists accept that blockchain development is the missing associate with settle sanctuary, assurance, and immovable quality concerns in the IoT and can be the silver slug essential through the IoT business. It will in general be used in following billions of related contraptions, enable the getting ready of trades and management between devices, and mull over colossal save assets to IoT industry makers. This decentralized technique would crash single motivations behind

Fig. 7 Blockchain in IoT

frustration, making a more grounded organic framework for contraptions to run on. The cryptographic figurings used by blockchains determine to make client data more secretive (Fig. 7).

The record used in blockchain is deliberately structured and cannot be constrained by threatening performers since it doesn't exist in any single region, and man-in-the-middle attacks can't be masterminded because there is no particular string of messages that can be caught. Blockchain makes trustless, shared advising possible and has quite recently exhibited its incentive in the domain of cash-related organizations through cryptographic types of cash, for instance, Bitcoin, giving guaranteed disseminated portion organizations without the necessity for pariah agents, upsetting what we call FinTech.

The decentralized, self-administering, and trust fewer limits of the blockchain make it an ideal part to transform into a basic segment of IoT courses of action. It is not unforeseen that adventure IoT headways have promptly gotten one of the early adopters of blockchain development.

Blockchain can keep an undisputable document of the authentic background of IoT splendid contraptions. This component enables the free working of keen contraptions without the prerequisite for the united force. Along these lines, the blockchain clears the path for a movement of IoT circumstances that were extraordinarily inconvenient or even hard to execute without it.

For example, through using the blockchain, IoT courses of action can enable protected illuminating between contraptions in an IoT sort out. In this model, the blockchain will give message exchanges between contraptions like money-related trades in a Bitcoin sort out. To engage message exchanges, devices will utilize splendid understandings which by then model the comprehension between the two social affairs.

One of the most invigorating limits of the blockchain is the ability to keep up an appropriately decentralized, accepted document of all trades occurring in a framework. This capacity is fundamental to enable the various compliances and

regulatory requirements of present-day IoT applications, for example, deprived of the need to rely upon a united model.

In summary, the main advantages of utilizing blockchain advancement in making sure about It can be abbreviated in three focuses: manufacture faith, decrease expenses, and quicken exchanges.

10.3 Challenges of Blockchain in IOT

Regardless of all of its preferences, the blockchain model isn't without its deformities and shortcomings:

- Scalability issues; Describe to the size of the blockchain document that may provoke concentration as it's created after a certain time and necessary a document the load up which is anticipating a shadow over the possible destiny of the blockchain development.
- Processing power and time: necessary to accomplish encryption counts for all the things drew in with blockchain-based IoT organic framework given the way that IoT situations are different and contained contraptions that have by and large extraordinary figuring capacities, and only one out of every odd one of them will be good for running a comparable encryption estimation at the perfect speed.
- Storage will be a deterrent: blockchain sheds the necessity for a central laborer to store trades and device IDs, anyway the record must be taken care of on the center points themselves, and the record will augment in size as time goes on. That is past the capacities of a wide extent of splendid contraptions, for instance, sensors, which have a low amassing limit.
- Lack of aptitudes: relatively few people perceive how blockchain development works and when you add IoT to the mix that number will drawback drastically, making a troublesome task in utilizing the essential gatherings to administrate and run blockchain adventures.
- Permitted and consistent issues: it's an additional area in all edges with no legal or consistent perspectives to follow, which speaks to a troublesome issue for IoT makers and organization providers. This test alone will startle away various associations from using blockchain advancement (Fig. 8).

10.4 The Optimum Secure IoT Model

Working up a protected model for the Internet of Things requires uncommon participation, management, and system for each piece of IoT natural framework. All contraptions must coordinate and be consolidated with every other device; all devices must bestow and work together faultlessly with related systems and establishments. Making such a model is possible; anyway it will in general be expensive, dreary, and irksome.

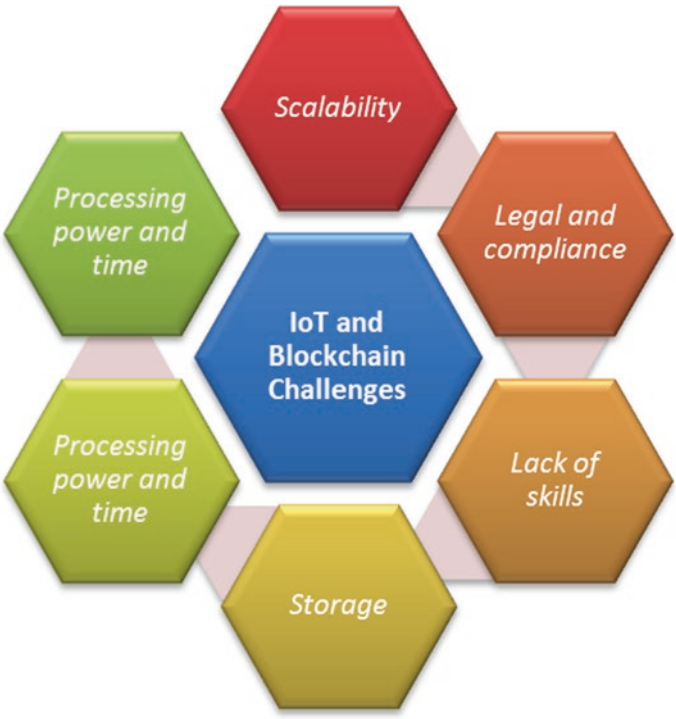


Fig. 8 IoT and blockchain challenges

Through the objective for us to achieve that perfect secure model of IoT, security ought to be worked in as the foundation of IoT condition, with exhaustive authenticity checks, approval, data affirmation, and all the data ought to be encoded at all levels. For example, at the presentation level, software development improvement affiliations ought to be better at forming code that is consistent, solid, and trustworthy, with unmatched code progression standards, getting ready, and risk examination and testing. Deprived of a solid base top structure, we will make more threats with every device added to the IoT. What we need is a protected and safe IoT with security guaranteed. That is a serious trade-off anyway not attainable, and blockchain development is an engaging decision if we can overcome its detriments.

11 Conclusion

Associations actualizing IoT arrangements keep on encountering difficulties recognizing security advances and approaches adequate to alleviate one-of-a-kind dangers to IoTs. Blockchain innovation vows to assume a significant job intending to these difficulties. Special security traders will start to offer these administrations,

yet it is conceivable to exploit promptly of the uprightness and legitimacy administrations given by blockchain implementations. We have featured highlights to consider when endeavoring to make sure about associated gadgets utilizing blockchain innovation. However, because of equipment restrictions of IoT, we reason that in a setting of a few hundred thousand or more IoT gadgets, a considerable lot of these gadgets couldn't fill in as exchange hubs (producing exchanges, giving agreement, and so forth.) and consequently would fall outside the safe blockchain. Numerous gadgets will profit by the security and different highlights offered by blockchain administrations through APIs from upstream exchange hubs of systems or by particular middle people. Those upstream abilities can be utilized to make sure about IoT gadgets (arrangement and update control, secure firmware update) and correspondences (IoT disclosure, confided in correspondence, message validation/marking). We trust this record rouses business pioneers and designers grasping the blockchain chance to broaden the abilities of this innovation to make sure about the Internet of Things.

References

1. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
2. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195
3. S.R. Kumar, N. Gayathri, S. Muthuramalingam, B. Balamurugan, C. Ramesh, M.K. Nallakaruppan, Medical big data mining and processing in e-Healthcare, in *Internet of Things in Biomedical Engineering*, (Academic Press, Amsterdam, 2019), pp. 323–339
4. P. Dhingra, N. Gayathri, S.R. Kumar, V. Singanamalla, C. Ramesh, B. Balamurugan, Internet of Things–based pharmaceutics data analysis, in *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*, (Academic Press, Amsterdam, 2020), pp. 85–131
5. S. Muthuramalingam, A. Bharathi, N. Gayathri, R. Sathiyaraj, B. Balamurugan, IoT based intelligent transportation system (IoT-ITS) for global perspective: a case study, in *Internet of Things and Big Data Analytics for Smart Generation*, (Springer, Cham, 2019), pp. 279–300
6. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 blockchain databases 2, in *Blockchain, Big Data and Machine Learning: Trends and Applications*, (2020), p. 97
7. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global, 2021), pp. 165–177
8. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, Boca Raton, 2020)

A Real-Time Monitoring Tool for Analyzing Ethereum Digital Currency in Global Business Transaction

K. Logu, T. Devi, N. Deepa, N. Gayathri, and S. Rakesh kumar

Abstract Ethereum (ETH) is a cryptocurrency system based on open-source blockchain technology to create a modern electronic cash transaction in decentralized network. Each node in Ethereum has an Ethereum Virtual Machine (EVM) that executes the HRPLs, similar to how Bitcoin's structure works. Now that the Ethereum price depends on market demand, we have to identify the day-to-day ETH market price to purchase a product or perform a business transaction in Cryptocurrency Security Standard (CCSS). Digital banking services like visa and Mastercard are having difficulties accessing remote and rural areas. Our proposed work is an automated intrusion detection (AID) tool that visualizes data from the ETH blockchain in a chart structure for tracing, tracking, and clustering. We focus on the number of transactions and current ETH value in the network using the AID tool. It is easy to convert ETH value into dollars using a consensus algorithm and human-readable programming language (HRPL).

Keywords AID · ETH · HRPL · Blockchain · Bitcoin

1 Introduction

Ethereum (ETH), the cryptographic cash of the Ethereum association, is apparently the second most standard automated token following Bitcoin (BTC). Without a doubt, it is the second-largest cryptographic cash based on market cap, and assessments between Ethereum and BTC are simply ordinary. Ethereum

K. Logu (✉) · T. Devi · N. Deepa
Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
e-mail: devit.sse@saveetha.com; ndeepa.sse@saveetha.com

N. Gayathri · S. Rakesh kumar
School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_8

and Bitcoin are similar from various perspectives: both are mechanized cash that can be traded via online exchanges as well as deposited among several types of advanced money wallets. Decentralization is the important feature of both tokens, as the containment is done with the help of a public bank. The use of cryptocurrency mentioned above culminated in the development of a record-keeping system known as blockchain. In any case, there are furthermore various fundamental capabilities between the two most notable computerized monetary forms by market cap. Below, we'll look at the comparable qualities and differentiations between Bitcoin and Ethereum.

Bitcoin was dispatched in the month of January 2009. It was introduced for shrewdly well-considered set in between white paper by the perplexing Satoshi Nakamoto BTCINR coin which offers the assurance to transfer online money that is ensured with no central place and at all take authority over financial principles. There are no physical bitcoins; instead, there are balances related with an open record that is cryptographically protected. Regardless of the fact that Bitcoin was not the essential undertaking at an online money of this sort, it was the best in its underlying undertakings, and it has come to be known as an original in one way or another to basically all computerized monetary standards which have been made over the previous decade. Over the long haul, the possibility of a virtual, decentralized money has gotten affirmation among regulators and government bodies. Disregarding the way that is definitely not an authoritatively seen method of portion or store of critical worth, advanced cash has sorted out some way to remove a claim to fame for itself and continues agreeing with the money-related system despite being reliably explored and examined. A blockchain advancement is being used to make applications that go past engaging an automated cash. Dispatched on the month of July 2015, Ethereum is the greatest and most grounded, open-completed decentralized programming stage. Ethereum engages the sending of HRPLs and decentralized applications (dapps) to be built and run with no excursion, distortion, control, or impedance from an untouchable. Ethereum comes all out with its own programming language which runs on a blockchain, enabling designers to build and run passed on applications. The normal uses of Ethereum are wide-going and are powered by its neighborhood cryptographic token, ether (consistently reduced as ETH). In 2014, Ethereum dispatched a presale for ether, which got a stunning response[1]. Ether looks like the fuel for running requests on the Ethereum stage and is used by originators to manufacture and run applications on the stage.

Ether is used overwhelmingly for two purposes: it is traded as a high-level cash on exchanges in a comparative plan as other computerized monetary standards, and it is used on the Ethereum association to run applications. According to Ethereum, "people wherever on the world use ETH to make portions, as a store of critical worth, or as security." While both Bitcoin and Ethereum networks are powered by the norm of scattered records and cryptography, the two

indeed differ in many ways. For example, trades on the Ethereum association may contain executable code, while data connected to Bitcoin network trades are generally only for keeping notes. Various differences fuse square time (an ether trade is confirmed in seconds as opposed to minutes for Bitcoin) and the process that they run on. Even more fundamentally, be that as it may, the Bitcoin and Ethereum networks are particular with respect to their overall focuses [5]. While Bitcoin was made as an alternative as opposed to public financial norms and likewise attempts to be a component of exchange and a store of critical worth, Ethereum was proposed as a phase to energize immutable, programmed arrangements and applications by methods for its own cash. Although BTC and ETH are both mechanized money-related guidelines, the primary job of ether isn't to develop itself as an alternative monetary system yet rather to empower and adjust the action of the Ethereum HRPL and dapp stage.

Ethereum is another usage case for a blockchain that supports the Bitcoin association, and theoretically should not, for the most part, fight with Bitcoin. Regardless, the reputation of ether has driven it into contention with every computerized money, especially from the perspective of vendors. For a huge part of its arrangement of encounters since the mid-2015 dispatch, ether has been close behind Bitcoin in rankings of the top computerized types of cash by market cap[12]. That being said, it's important to note that the ether climate is much more unassuming than Bitcoin's. As of January 2020, ether's market cap is barely short of $6 billion, while Bitcoin's market cap is practically on different occasions more than $147 billion.

Ethereum isn't asserted by anyone. The whole of the tasks and organizations associated with the association requires enlisting power—and that power isn't free. Ether is the response for the issue of portion—a high-level asset transporter like a bond or other security. You can think of it as the advanced cash of the Ethereum network. Much equivalent to cash, it needn't bother with an untouchable to gauge or support trades. According to ethereum.org, it ought to be considered as fuel for the applications on the decentralized Ethereum network. This is a hypothetical technique for sketching out ether's ability, and a strong model may help with making things more understood. Assume there is an application on the Ethereum network that grants you to make, change, and eradicate clear notes. To complete any of these endeavors, the application requires taking care of intensity by methods for the association. To deal with the cost of this power, you presumably need to pay an insignificant charge at whatever point you wish to reveal any enhancements to your present notes. Ether is the token by which you make this portion. It is, in a manner of speaking, progressed oil in that it allows the association to manage the movements you've made. As such a fuel, it by then looks good that ether trade costs will be assorted depending on how much fuel is required for the organization.

2 Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) is a ground-breaking, sandboxed virtual stack implanted inside each full Ethereum hub, liable for executing contract bytecode. Agreements are normally written in more significant level dialects, similar to Solidity, at which point ordered to EVM bytecode. This implies that the machine code is totally separated from the organization, filesystem, or any cycles of the host PC. Each hub in the Ethereum network runs an EVM occurrence which permits them to concur on executing similar guidelines[2]. The EVM is Turing-complete, which alludes to a framework equipped for playing out any legitimate advance of a computational capacity. JavaScript, the programming language which controls the overall web, generally utilizes Turing completeness.

The EVM is basic to the Ethereum protocol and is instrumental to the agreement motor of the Ethereum framework. It permits anybody to execute code in a trustless biological system in which the result of an execution can be ensured and is completely deterministic (i.e., executing HRPLs). For each guidance actualized on the EVM, a framework that monitors execution cost relegates to the guidance a related expense in gas units. At the point when a client needs to start an execution, they hold some ether, which they are eager to pay for this gas cost. By utilizing the gas system, two significant issues are addressed: a validator is ensured to get the underlying prepaid sum, regardless of whether the execution falls flat[8]. An execution can't run longer than the prepaid sum would permit. Rather than circling inconclusively, the execution would continue until it runs empty. The EVM accomplishes Turing completeness by empowering an economy that charges for every product guidance executed rather than per monetary exchange executed like Bitcoin does. Rather than an exchange expense, you have a sort of charge for running projects.

Being Turing-complete implies that Ethereum is actually a broadly distributed useful overall PC and could even predict the elements of the web as we know it. Ethereum could empower us to make document-sharing economies, distributed crowdfunding occasions, HRPLs, markets for leasing the unused hard-drive space on your PC, a disintermediated Uber or Facebook (the items without the organizations), and so on. It's fundamentally similar to the web in 1994: nobody understands what the future will bring. The Ethereum convention itself exists exclusively to keep the nonstop, continuous, and unchanging activity of this unique state machine[7]. It's the climate in which all Ethereum records and HRPLs live. At some random square in the chain, Ethereum has one and only one "authoritative" state, and the EVM is what characterizes the principles for processing another legitimate state from square to hinder.

2.1 The Ethereum State Transition Function

The EVM carries on as a numerical capacity would: given an information, it creates a deterministic yield. It accordingly is very useful to all the more officially depict Ethereum as having a state progress work:

$$Y\left(S,T\right) = S' \tag{1}$$

Given an old legitimate state (S) and another arrangement of substantial exchanges (T), the Ethereum state change work $Y(S, T)$ creates another substantial yield state S'.

2.1.1 State

Ethereum regarding state is a vast information structure known as an adjusted Merkle Patricia Trie, which keeps all records connected by hashes and reducible to a solitary root hash put away on the blockchain.

2.1.2 Transactions

Exchanges are cryptographically marked directions from accounts. There are two sorts of exchanges: those which bring about message calls and those which bring about agreement creation. Agreement creation brings about the formation of another agreement account containing aggregated HRPL bytecode. At whatever point another record settles on a message decision to that agreement, it executes its bytecode.

2.1.3 Vapor and EVM Bytecode

On Ethereum, vapor can be considered as being identical to an expense. Each and every exchange that is performed on the Ethereum network necessitates that a charge be appended to it, which is paid as gas. The idea of Ethereum's gas can be divided into two categories:

- Vapor—Serves as an instrument by which we measure the expenses that will be needed for a specific calculation to be executed.
- Vapor Price—This is the measure of ether that an individual is happy to spend on each unit of gas. Gas cost is frequently estimated in "Wei", which is the littlest unit of ether, where 10^18 Wei speaks to one ether.

In this way, in order for a person to execute an exchange on the Ethereum organization, the sender should set the gas value associated with the exchange as far as possible. If a sender doesn't have the necessary gas to play out an exchange, at that point, it is said to be running on empty and invalid.

Vapor can restrict the quantity of calculations that can be performed by the Ethereum Virtual Machine in a couple of ways, including:

- Blocks that are mined on the Ethereum blockchain have a gas limit joined to them, so the proportion of gas used by all trades inside a square can't outperform a particular entirety.

Connected to gas is the gas esteem, and regardless of whether gas limit constraints were lifted and the machine was theoretically prepared to handle any trouble it got, a couple of trades may be exorbitantly complicated and exhibit monetarily outlandish.

The Ethereum Virtual Machine has its own programming language, known as the "EVM bytecode." Right when the code is written in higher-level programming languages, for instance, Ethereum's understanding on object-oriented programming language Solidity, this code can be translated to EVM bytecode, so that the Ethereum Virtual Machine can fathom what has been formed.

2.1.4 Transaction-Based State Machine

The Ethereum Virtual Machine is a huge part of the Ethereum advancement, since it is the subject for dealing with inside state and estimation on the association. The machine ought to moreover manage account information such as addresses, balances, current gas cost, and square information. As referred to previously, the Ethereum Virtual Machine is responsible for dealing with inward state on the association. The machine should screen the status of different parts to successfully maintain a trade[10]. This is huge because it is the state of these parts that genuinely drives the level of progress in the general blockchain. This is the explanation Ethereum is much of the time portrayed the same as a trade-based state machine. Before we look at the changed parts that the Ethereum Virtual Machine should screen, a short explanation of the possibility of a "state" may be significant.

In the field of computer programming, a state machine suggests a machine that can scrutinize the movement of information sources and, taking into account those data sources, change to another state[11]. Basically, Ethereum's state machine moreover works along these lines. Before any data sources are made, or before any trades on Ethereum are executed, the early phase is something of a reasonable record. As trades on the association are done, any point during this time implies the current status of Ethereum. In order for a state progress to occur, trades must be authentic, and a trade is considered as significant when it is viably endorsed through the mining cycle. This mining cycle is known as proof of work (PoW), and it remembers center points for the Ethereum network utilizing PC resources for the benefit of making a square of significant trades and adding it to the blockchain.

A digger can add a square to the blockchain when they can give a mathematical "affirmation." A significant confirmation signals to the association that the square is genuine, allowing it to be recognized and added to the chain. An earthmover, who adequately favors a square, is repaid with Ethereum's neighborhood asset, ether, as a trade-off for depleting enlisting resources during the PoW cycle.

2.1.5 Account State

Ethereum can be considered as including different little records that are good for interfacing with one another (this is possible taking into account Ethereum's message-passing packaging work). Records on Ethereum can be divided into:

- Distantly guaranteed records—These records are compelled by private keys and have no code related with them.
- Arrangement accounts—These records are obliged by their arrangement code and have code related with them.

A record that is distantly guaranteed can send messages to other distantly guaranteed records, or other understanding records. This is done via cautiously denoting a trade by the use of a private key. Correspondence between two distantly guaranteed records can be seen as fundamentally being a trade of critical worth. Nevertheless, a message between a distantly guaranteed account and an understanding record has the effect of executing the arrangement record's code. This enables the understanding record to perform exercises that are spread out in the code, which can include token trade, arrangement of new tokens, etc. Note that arrangement accounts can't begin another trade in isolation (as opposed to distantly guaranteed accounts). Arrangement accounts are responsive in the sense that they can simply take an interest in trades that fill in as a response to various trades that they have gotten, which can be from a distantly guaranteed record or from other understanding records.

3 Cryptocurrency Security Standard (CCSS)

Maybe the best trial of open decentralized is sureness. Persons in affiliations are stressed over through approval from authorization or possibly order limitations of cryptographic cash trades. Such requirements are correct, currently defeating the choice speed of micropayment. By normalizing the protected systems and strategies used by Litecoin structures around the world, end users have the choice to make even more successful decisions about the things and organizations they can use or associations they wish to change[13]. On the other hand, various cryptopayments, as protected, are not spoken to by a central control point or "authenticate"; normalizing on security will be a troublesome cycle. Basic approaches to manage in a protected environment will come from micropayments that grasp authorized record

frameworks, for instance, rippled XRP. In authorized record conditions, while learning approvals may be public or kept to an emotional degree, created assents are held together in one affiliation. Taking everything into account, normalizing on protected mode is more feasible.

The Payment Card Industry Data Security Standard (PCI DSS) can be mostly credited for the accomplishment of web portions that should be standard or fatal in financial structures[3]. A current standard was driven in critical portion marks, for instance, American Express, Discover Financial Services, JCB International, Mastercard, and Visa Inc.; in addition, it must become the de facto structure for affiliations that manage or store Mastercard nuances. Defiance to this standard suggests that an affiliation won't have the choice to lead online portions utilizing visas.

A secure standard in the crypto space, commonly referred as Cryptocurrency Security Standard, was well-known for ensuring coin organization. The basic is present in go-to approval for any information system that manages and directs wallets as part of its industry reasoning.

CCSS is an open-based protocol based on advanced money storage methods used within an organization. It is expected that CCSS will be used to expand basic information security practices and to enhanced standards (ISO 27001, PCI, etc.), but it will not be able to replace them[12]. The CCSS cannot be diverged from PCI DSS as an equal standard. Despite the fact that the PCI DSS basic extends to the entire trade stream (e.g., from the development used to pick up trades to how the information in the trade is dealt across all methods of setup), the CCSS standard doesn't give a comparable incorporation and instead focuses on the protected organization of the web wallets. In addition to well-being endeavors, it will be important to ensure the conditions under which the online-protected fragments work.

3.1 Cryptocurrency Wallets

A wallet is a combination of public location and private key. The wallets can be arranged based on the strategy and area of capacity in the accompanying sections.

3.1.1 Hot and Cold Wallets

Web network characterizes a wallet regarding hot or cold. Hot wallets are associated with the Internet, making them less secure and posing more dangers while still being easy to use. Cold wallets, on the other hand, are put away disconnected and don't need web network, in this manner improving security and posing less danger. When contrasted with a safe or a vault, more generous amounts of cash can be put away than that in a heft around a wallet. Hot wallets are bound to be utilized for

day-to-day exchanges, while cold wallets will be used for more long-term investments. Hot wallets are anything but difficult to set up, and the assets are rapidly open. Dealers make good use of them. Cold wallets are hack-safe, and accordingly the cool stockpiling is reasonable for HODLers. As a security technique, just a little percent is put away in hot wallets while having the option to exchange straightforwardly from their cool stockpiling gadgets.

3.1.2 Hardware Wallets

Equipment wallets are equipment gadgets that exclusively handle public locations and keys. It would seem a USB with an OLED screen and side catches. It is a battery-less gadget that can be connected to a PC and accessed by local work area applications. It cost as much as 70–150 dollars; however it is justified, despite any trouble. They have gotten a blended reaction. They are safer than hot wallets and more user-friendly than paper wallets, but not as much as web and work area wallets. They are accessible in various structures and offer sensible measures of control. They are hard for amateurs to utilize when the speculation is critical. Most famous equipment wallets are Ledger Nano S and Trezor.

3.1.3 Paper Wallets

It is a truly printed QR-coded structure wallet. A few wallets permit downloading the code to create new locations that are disconnected. They are not inclined to hacks, but rather the quantity of defects has made them hazardous. A significant defect isn't having the option to send incomplete assets. Hence, it can't be reused. They used to be famous for cold stockpiling, but that changed after the introduction of equipment wallets. All things considered, in the event that tough security insurances are taken, at that point, paper wallets can be set up.

3.1.4 Desktop Wallets

These are installable programming packs accessible for working frameworks and are getting genuine with time. Hostile to infection is required in light of the fact that a framework associated with the Internet presents central security issues. Rather than keeping cryptos on a trade, work area wallets for bitcoins should be utilized. They are the third most secure approach to store digital forms of money and the best technique for cold stockpiling in a totally spotless framework. They are anything but difficult to utilize, give protection, are anonymous, and include no outsider. Standard sponsorship of the PC is required. Mainstream work area wallets are Exodus, Bitcoin center, Electrum, and so forth.

3.1.5 Mobile Wallets

Portable wallets are much the same as work area wallets made for cell phones. They are very advantageous as they utilize QR codes for exchanges. They are reasonable for day-to-day tasks but are defenseless against malware contamination. Encryption of versatile wallets is fundamental. They are cost-effective and easy to use, but they are prone to infections. Some versatile wallets are Coinomi and Mycelium.

3.1.6 Web Wallets

As the name proposes, these wallets are accessed through web programs. The private keys are held in some web wallets and are inclined to distributed denial-of-service (DDOS) assaults. They can be facilitated or non-facilitated. Non-facilitated is favored as assets are consistently in charge. They are the most unsecure wallets. They are not equivalent to hot wallets. They are ideal for little ventures and permit fast exchanges. A portion of these are MetaMask and Coinbase.

3.1.7 Takeaway

You can pick the wallet according to your requirements, just make sure to back it up routinely and utilize the most recent programming. If you are keen on learning more, you can pursue cryptographic money confirmations or digital currency affirmation course on the web.

4 Consensus Algorithms

To refresh the record, the organization needs to come to agreement through a calculation. Showing up at an agreement on a disseminated network implies that everybody concedes to the present status of the record (e.g., how much cash does each record have) and affirms that nobody is twofold going through their cash. Coming to an agreement is a software engineering issue in shortcoming open-minded dispersed frameworks. Creating an agreement implies that numerous workers on the appropriated network concede to the current truth condition of the framework or, in the essential blockchain case, the values in the record. When the organization PCs arrive at a choice on a worth, that choice is conclusive. In the old-style software engineering setting, agreement calculations are utilized to concur on the orders in the logs of the disseminated workers. In blockchain organizations, the three principle sorts of agreement calculations for showing up at agreement in a circulated way are Double Verification of Work (DVOW), Double Verification of Stake (DVOS), and Advanced Verification Byzantine Fault Tolerance (AVBFT). The fundamental advancement of the blockchain convention is the blockchain information structure

on top of an agreement calculation, which makes it conceivable to assemble an open dispersed organization in which the entirety of the gatherings can agree.

In POW agreement, the calculations that work the dispersed framework reward excavators (customer machines on the framework) who take care of numerical issues. New exchanges executed on the organization are steered from the product wallets executing them to the entirety of the mining customers on the organization. In Bitcoin, for instance, each mining customer has a memory pool (mempool) to gather approaching unsubstantiated exchanges. The mining programming approves the new exchanges and clumps them into a square (every 10 min in Bitcoin and each ~12 s in Ethereum). The monetary impetus for each mining customer is to be the one to make the new square of exchanges that different machines will all take as the new truth condition of the arrangement and attach to the decentralized duplicate of the blockchain they keep up on their companion hub. It is rewarding to record these exchanges ("find a square" or "mine a square"), and accordingly many committed mining tasks (running custom ASICs) exist for Bitcoin. Evidences of work agreement components are condemned for the inefficient utilization of calculation to deliver the cryptosecurity.

In POS, the agreement calculation is rather founded on possessing a stake in the organization. In POS frameworks, the maker of another square is picked in a deterministic manner, contingent upon its stake or level of responsibility (riches) in the organization. Notwithstanding, POS frameworks are maybe superfluously tangled with casting ballot levels and are not really more effective than Bitcoin as far as what may be viewed as inefficient calculation. Subsequently, a portion of the cutting-edge blockchains are thinking about PBFT as a more drawn-out term arrangement that would permit one million appropriated machines (customers) on an organization to meet up in a typical and secure truth condition of the framework. PBFT is the capacity of an appropriated process framework to work independent of defective hubs (malignant or something else). PBFT depends on a variety of members on the appropriate framework (200 or 300). For each square of exchanges, calculations haphazardly select a little after gathering clients in a protected and reasonable manner. To shield them from aggressors, the characters of these clients are typically covered up until the square is affirmed. The size of this gathering ordinarily stays consistent as the organization develops. For instance, 250 of 300 machines (picked aimlessly per the algorithmic framework) would have to sign any exchange whether there are 1000 or 1,000,000 hubs on the organization. DFINITY and Algorand are instances of cutting-edge blockchain projects with PBFT agreement calculations.

4.1 Double Verification of Stake (DVOS)

DVOS is a philosophy in DVOW that requires less CPU process for mining the data. Regardless of the way that this is moreover a count, and the item is same as DVOW, the cycle is extraordinary here. As if there ought to emerge an event of DVOW

where a digger is remunerated by settling mathematical issues and making new squares, in DVOS, the creator of another square must pick by deterministic process, dependent upon the health, similarly taken as stake. Through collection of information to be DVOS part, there is no square prize. Along these lines, the backhoes take the trade charges. DVOS instrument has its own potential gains and disadvantages, and the real use is extremely complicated:

$$K\_t(ij) = \max : K\_t - 1 * a(i,j) * b\_j(O\_t) \tag{2}$$

where

- *K_t*(*ij*) is the past Viterbi way likelihood from the past time step.
- *aij* is the progress likelihood from past state *qi* to present status *qj*.
- *bj*(*Ot*) is the state perception probability of the perception image *ot* given the present status *j*.

4.2 Advanced Verification of Stake (AVOS)

AVOS is not the same as DVOS in any way. Here, the token holder does not work on the authenticity in squares without assistance from any other person, yet they select agents to do the endorsement for them. In an AVOS structure, there are generally between 21 and 100 picked turnovers. The picked turnovers are being changed infrequently based on a designated solicitation in passed on squares. In this case, you must have a low number of specialists, and grants must be capable and make arranged clock-based designations to disperse blocks. In case the specialists miss their squares reliably or convey invalid trades, the representative paused voters can opt out and move to a different picked turnover. Not under any condition like DVOW and DVOS, in AVOS, diggers can cooperate to make Litecoin. With a communitarian-dominated thinking cycle, DVOS has a choice to run critical degrees at a faster pace than other arrangement counts.

4.3 Byzantine Fault Tolerance (BFT)

The term “Byzantine fault tolerance” (BFT) is derived from a response to “Byzantine commandants’ anxiety.” BFT can be used to fix the issue on radical or faulty center point. A person from the organization is clashing information to other traders, the resolute nature of the blockchain isolates, and there is no central position to address. In conclusion, DVOW as of now offers BFT through dealing with energy. On the other hand, DVOS should have a more certain plan. Center points will regularly project a polling form to recognize the real trade. The more

promising type of DVOS on works with BFT should manage preferring trades in the block technology.

4.4 Advanced Byzantine Fault Tolerance (ABFT)

To understand estimations, ABFT is set up to manage non-deterministic chain-based execution. AVBFT is a chief response for more arrangements if there ought to be an event of Byzantine dissatisfaction. Glorious and Ripple moreover use AVBFT. In an AVBFT instrument, each "general" term in an internal state advances data status. Resulting to tolerating information, general information are used with the inside state to start a process cycle. A count cycle gets some data about the appraisal on the message. In the wake of showing up at a goal, the general offers to make a decision from various leaders of the system. Understanding information is reliant on, without a doubt, the quantity of decisions introduced by the officials. It controls a low-weighted display in a copied organization:

$$n = 3f + 1,$$

$$f = \frac{n-1}{3} \tag{3}$$

Three periods of comprehension among the four centers are portrayed, where Node 4 is the defective center and Nodes 1–3 are the standard centers. In any case, the client begins sales, and resulting to getting the sales, Node 1 sends a preprepared message to various centers. If various centers agree to the request, they will enter the prepare stage; else, they will send an excusal message back. In the prepare stage, if preprepared messages are gotten from more than 2f centers, the availability will be done, and the submit stage will be entered. In the submit stage, the submit information is conveyed to various center points. At whatever point submitted messages are gotten from more than 2f centers, the submit stage will be done, and most of the center points will concur. Finally, the information will be offered an explanation to the client before it is dealt with. The estimation has set a relating time detail for each framework during the time spent concurring. If the task of this stage fails to be done inside the foreordained time, the current round of understanding closes for break.

4.5 SIEVE

Sifter agreement components used by hyper-material allow the association and distinguish and dispose possible non-deterministic sales, besides achieving concurrence to yield suggesting trades.

4.6 Verification of Force (VOF)

VOF is a wide gathering of understanding computations based on relevant Algorand arrangement model. Right when VOS, the degree of coin asserted, is associated with the probability of "finding" an accompanying square, random tolerably weighted worth is being used. Filecoin's Verification the Space time is weighted on the sum of IPFS information being taken care of. To find small distinct system join loads are products like Double Verification the Reputation:

$$\begin{cases} \text{hash}(T) = \text{hash value}, \\ \text{verification (hash value} \geq \text{target} \end{cases} \tag{4}$$

The DVOW estimation is a process heightened count that eats up broad energy and resources. Reliably, the Bitcoin network consumes about 57.6 TWh of intensity, indistinguishable from the yearly force use of Srilanka. Additionally, the obstruction for Bitcoin mining is proceeding, suggesting that more vital power will be consumed. Despite its epic energy utilization, this instrument can ensure the security and trust of information. Unmistakably, the POW calculation has some other regular distortions. The tremendous energy use prompts a low level of individual support and changes the Bitcoin network into a different leveled or operational mining pool. Suitably, the Bitcoin network steadily will be joined when everything is said and done, despite the chief thought about decentralization:

$$D(l) = D\left(\sum_i l_i\right) = \sum_i D(l_i). \tag{5}$$

During the time spent forking, the most elevated blockchain is the one with the best complete trouble, as seen in the accompanying condition:

$$\varnothing(l_1, l_2, \ldots . l_n) = l_m, \text{where } m = \arg\max_{i \in 1,\ldots n}\left(D(l_i)\right) \tag{6}$$

4.7 Unique Node Lists (UNL)

Wave uses "all in all confided in sub-organizations" agreement calculations called "Unique Node Lists" (UNL) to manage high inertness, which typically portrays BFT-lenient frameworks. To arrive at an agreement, a hub needs to ask its own UNL instead of the whole organization.

4.8 Verification of Light (VOL)

In Verification of Light, instead of wasting money on costly PC gear, "consumer" coins should be sent to an unrecoverable location. It can acquire a regular advantage to mining technique on a framework dependent on a regular choice cycle. Excavators can consume the local money or hand cash in elective coin. The more Litecoin you consume, the higher your chances of mining in the following square. If your stake in the framework falls flat, you will need to consume more coins to expand your chances of being chosen for the following square. VOL is a decent option for PoW, in spite of fact that the convention squanders assets. Litecoin is a solitary coin that uses Verification of Light. Litecoin utilizes through a mix of DVOW, DVOS, and DVOB.

4.9 Double Verification of Activity (DVOA)

DVOA should be designed using elective motivator through various Litecoin diggers. This consolidates both DVOW and DVOS. In DVOA, diggers start by addressing the riddle in a DVOW manner. In the event that the squares mined don't contain any exchanges, the framework changes to POS. In view of the header data, a gathering of validators is relegated to assign the new square. If a validator claims more coins, he has the most noteworthy opportunity to be picked. When all the chosen validators sign, the layout turns into a square.

4.10 Double Verification of Capacity (DVOC)

The ability to arrange a computation framework is remarkable according to others. You pay for all of the harder circle periods. In more difficult times, the chances of different changes are more likely to occur, so you will mine the going with square and gain. Before compressing in a DVOTC, in count delivers on a large number of educational records known as "plots," you can save on your own storage drive. Considerably, the more number of plots, the better the chances of finding the going with square. Then, using a different instrument, you need to invest energy for a marvelous course of action on storage drive space. Burst coin is the specific robotized cash that has a premium in cutoff:

$$\begin{aligned} &\text{minimum} \sum_{i=1+2} x_{i.j} \\ &\sum_{i.j} a_{ij} x_i \, x_j \;\; \beta \;\; k, \forall i \\ &\qquad y \ni \{0,1\}, \forall i \end{aligned} \tag{7}$$

Given the non-negative number parameters *k* and *d*, the legit Ethereum recognizable proof issue can be detailed as a maximum *k*-autonomous set issue in the *d*-dissension chart of the given square, denoted as DVOC-(*k*, *d*).

Algorithm 1 Consensus Algorithm

Input: the block ETH (n blocks),d, alpha

1. Begin
2. Initialize matrix D(n*n)
3. Initialize matrix M(n*n)
4. For blocks I,j do
5. $D[i,j] \leftarrow discord(i,j)$
6. EndFor
7. $S \leftarrow quantile(D, alpha)$
8. $While\ s > d\ do$
9. $M \leftarrow Zero\ martrix\ of\ the\ same$ dimension as D
10. For i,j do
11. $if\ D[i,j] > s\ do$
12. $M[i,j] \leftarrow 1$
13. Endif
14. EndFor
15. $h \leftarrow getMIS(M)$
16. $D \leftarrow D[h,h]$
17. $s \leftarrow quantile(D, alpha)$
18. EndWhile
19. $M \leftarrow zero\ matrix\ of\ the\ same\ dimension\ as\ D$
20. For i,j do
21. if D[i,j] > d do
22. $M[i,j] \leftarrow 1$
23. Endif
24. EndFor
25. $h \leftarrow getMIS(M)$
26. return h
27. End

5 Human-Readable Programming Language (HRPL)

We have two unmistakable sorts of records in Ethereum: distantly asserted records (EOAs) and arrangement accounts. EOAs are compelled by customers, often through programming, for instance, a wallet application that is external to the Ethereum stage. Strangely, contract accounts are obliged by a program code (furthermore normally implied as "HRPLs") that is executed by the Ethereum Virtual Machine. Along these lines, EOAs are direct records with no connected code or data amassing; however, contract accounts have both related code and data storing. EOAs are obliged by trades made and cryptographically embraced with a private key in "this current reality" external to and liberated from the show; however, contract accounts don't have private keys that accordingly "control themselves" in the predestined way suggested by their HRPL code. The two sorts of records are recognized by an Ethereum address[6]. In this part, we will inspect contract accounts and the program code that controls them.

The term HRPL has been used over time to portray a wide scope of things. During the 1990s, cryptographer Nick Szabo established the term and portrayed it as "a lot of ensures, demonstrated in cutting edge structure, including shows inside which the social occasions perform on various certifications." Since then, the possibility of HRPLs has grown, especially after the introduction of decentralized blockchain stages with the advancement of Bitcoin in 2009[4]. With respect to Ethereum, the term is a bit of a misnomer, given that Ethereum HRPLs are neither splendid nor real arrangements, but the term has stuck. In this book, we use the articulation "HRPLs" to insinuate lasting PC programs that run deterministically with respect to an Ethereum Virtual Machine as a component of the Ethereum network show.

PC Programs
Brilliant agreements are essentially PC programs. "Contract" has no legitimate significance in this specific situation.

Unchanging
When sent, the code of a savvy contract can't change. Dissimilar with customary programming, the best way to change a brilliant agreement is to send another occurrence.

Deterministic
The aftereffect of the execution of a keen agreement is comparable for every single person who runs it, given the setting of the trade that began its execution and the state of the Ethereum blockchain at the time of execution.

EVM Setting
Splendid arrangements work with an uncommonly confined execution setting. They can get to their own express, the setting of the trade that called them, and some information about the most recent squares.

Algorithm 2 HRPL Algorithm

$p_0 \leftarrow GeneticInitialSolution()$

$p \leftarrow Apply\ a\ value\ serach\ (p\ \ 0)$

While Not optimum and ETHCount < UnitEvals do

$t \leftarrow selectParents(p)$

NumETH = 0

While Not end of evolved sequence of time

do

AVply current sequence to t or p

If current measure is AVplied on t then

NumETH - NumETH + 1

end if

end while

ETHCount = ETHCount + NumETH

end while

Decentralized World PC

The EVM runs as a nearby case on each Ethereum hub, but since all examples of the EVM work on a similar starting state and produce a similar last express, the framework overall works as a solitary "world PC."

5.1 Ethereum High-Level Languages

The EVM is a virtual machine that runs an extraordinary kind of code called EVM bytecode, like your PC's CPU, which runs machine code, for instance, x86_64. We will examine the movement and language of the EVM. In this part, we will perceive how splendid arrangements are created to run on the EVM. While it is possible to program splendid arrangements directly in bytecode, EVM bytecode is genuinely badly designed and hard for programmers to scrutinize and appreciate. In light of everything, most Ethereum creators use a higher-level language to form programs and a compiler to change over them into bytecode.

While any higher-level language could be changed in accordance with creating smart arrangements, changing a self-confident language to be compilable to EVM bytecode is a huge awkward exercise and would, generally speaking, lead to some proportion of chaos. Keen arrangements work in an especially obliged and moderate execution atmosphere (the EVM)[9]. Furthermore, an excellent course of action of EVM-express system elements and limits should be available. In that limit, it is less complex to develop an insightful arrangement language without any planning than it is to make a generally valuable language sensible for making wise agreements. Thus, different specific explanation vernaculars have emerged for programming splendid arrangements. Ethereum has a couple of such vernaculars, alongside the compilers expected to convey EVM-executable bytecode.

When in doubt, programming tongues can be orchestrated into two extensive programming ideal models: illustrative and fundamental, in any case called utilitarian and procedural, independently. In illustrative programming, we form limits that express the reasoning of a program, but not its stream. Impactful composing PC programming is used to make programs with no outcomes, inferring that there are no movements to state outside of a limit. Conclusive programming lingos join Haskell and SQL[14]. Essential programming, then again, is where an engineer makes a pack out of techniques that combine the reasoning and stream of a program. Fundamental programming tongues join C++ and Java. A couple of tongues are "creamer," suggesting that they stimulate conclusive programming but can also be used to convey an essential programming perspective. Such half and parts fuse Lisp, JavaScript, and Python. Overall, any essential language can be used to write in a definitive perspective, yet it habitually achieves inelegant code. By connection, unadulterated brilliant tongues can't be used to write in an essential perspective. In totally logical lingos, there are no "factors."

While fundamental composing PC programming is even more consistently used by designers, it will in general be very difficult to create programs that execute decisively exactly as expected. The limit of any bit of the program to change the state of another makes it difficult to reason about a program's execution and presents various open entryways for bugs. Impactful programming, by assessment, makes it more clear how a program will act: since it has no outcomes, any bit of a program can be seen in separation.

In canny agreements, bugs from a genuine perspective cost money. Therefore, it is fundamentally critical to compose keen agreements without unintended impacts. To do that, you should have the option to unmistakably reason about the normal conduct of the program. Along these lines, decisive dialects assume a lot greater part in brilliant agreements than they do as a rule reason programming. In any case, as you will see, the most generally utilized language for shrewd agreements (Solidity) is basic. Software engineers, as most people, oppose change!

The most commonly used high-level programming dialects for savvy contracts (requested by rough age) are as follows.

5.1.1 LLL

A useful (definitive) programming language is Lisp-like language. It was the primary significant level language for Ethereum savvy contracts but is infrequently utilized today.

5.1.2 Serpent

Serpent is a procedural (basic) programming language with a linguistic structure like Python. It can likewise be utilized to compose useful (decisive) code; however, it isn't completely liberated from results.

5.1.3 Solidity

Solidity is a procedural (basic) programming language with a sentence structure like JavaScript, C++, or Java. It is the most well-known and often utilized language for Ethereum savvy contracts.

5.1.4 Vyper

Vyper is a more recently developed language, similar to Serpent and again with a Python-like sentence structure. It is proposed to draw nearer to an unadulterated useful Python-like language than Serpent, but not to supplant Serpent.

5.1.5 Bamboo

Bamboo is a recently evolved language, impacted by Erlang, with express state advances and without iterative streams (circles). It is planned to lessen results and increment review capacity. It is new but is to be generally embraced.

6 Simulation and Analysis

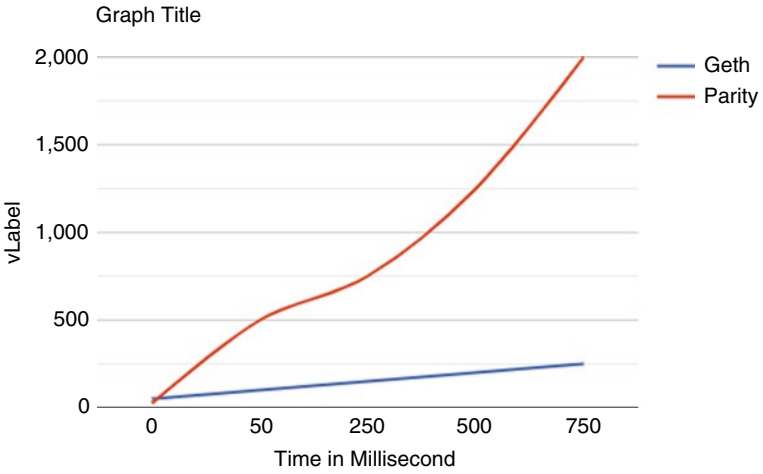


Fig. 1 Graph Shows comparsion between Geth and Parity in millisecond

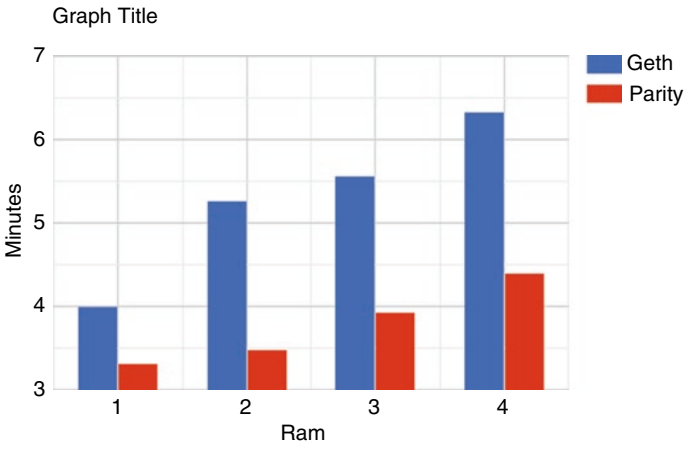


Fig. 2 Bar Graph shows time consumption between Geth and Parity in minutes

7 Conclusion

This paper provides the automated intrusion detection (AID) tool to visualize the data of ETH blockchain. Mostly, this tool is used for Ethereum (ETH). However, it can be modified with any Litecoin by adding appropriate module in its modular industry. This software is used for converting ETH to currency value and for transferring a secure ETH to various currencies like dollars, Dirham, etc. The results obtained using this software are encouraging. In the future, there will be various types of works to support the cryptocurrencies like TRON for blockchain analysis.

References

1. D. Patel, J. Bothra, V. Patel, Blockchain exhumed, in *2017 ISEA Asia Security and Privacy (ISEASP)*, (IEEE, 2017), pp. 1–12. https://doi.org/10.1109/ISEASP.2017.797699
2. N. Christin, Traveling the silk road: a measurement analysis of a large anonymous online marketplace, in *Proceedings of the 22nd International Conference on World Wide Web*, (IEEE, 2012), pp. 213–224
3. S. Foley, J.R. Karlsen, T.J. Putniņš, Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? Rev. Financ. Stud. **32**, 1798–1853 (2019). https://doi.org/10.1093/rfs/hhz015
4. D. Heaven, Sitting with the cyber-sleuths who track cryptocurrency criminals. MIT Technol. Rev. (2018). URL: https://www.technologyreview.com/s/610807/sitting-with-thecyber-sleuths-who-track-cryptocurrency-criminals/
5. S. Martins, Y. Yang, Introduction to bitcoins: a pseudoanonymous electronic currency system, in *Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research*, (IBM Corp., 2011), pp. 349–350
6. 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, Heidelberg, 2014), pp. 469–485. https://doi.org/10.1007/978-3-662-45472-5_30
7. F. Reid, M. Harrigan, An analysis of anonymity in the bitcoin system, in *Security and Privacy in Social Networks*, (Springer, New York, 2013), pp. 197–223
8. Zero to Monero: First Edition – a technical guide to a private digital currency; for beginners, amateurs, and experts (2018) URL: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf
9. E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash: decentralized anonymous payments from bitcoin. IEEE Symposium Secur. Privacy **2014**, 459–474 (2014)
10. J. Seo, M. Park, H. Oh, K. Lee, Money laundering in the bitcoin network: perspective of mixing services, in *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, (IEEE, 2018), pp. 1403–1405
11. M. Fleder, M.S. Kester, S. Pillai, Bitcoin transaction grAVh analysis. arXiv preprint arXiv:1502.01657 (2015)
12. D. Ermilov, M. Panovy, Y. Yanovich, Automatic bitcoin address clustering, in *16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, (IEEE, 2017), pp. 461–466
13. M. Jourdan et al., Characterizing entities in the bitcoin blockchain, in *2018 IEEE International Conference on Data Mining Workshops (ICDMW)*, (IEEE, 2018)
14. L. Cai, B. Wang, Research on tracking and tracing bitcoin fund flows, in *2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC).*, (IEEE, 2008). URL: https://bitcoin.org/bitcoin.pdf

Blockchain-Powered Healthcare Information Exchange Systems to Support Various Stakeholders

R. Ramya, A. Anandh, K. Muthulakshmi, S. Janani, and N. Gayathri

Abstract Initially, blockchain technology was emerged for the enhancement of financial transactions, as it is independent of the need to have any third party to verify the transactions. Progressively, it has been slightly modified based on the different application-specific requirements such as data security and privacy. One of the emerging applications of blockchain is E-healthcare that concerns mainly about integrity, authenticity, and consistency of patients' medical records. Due to the evolution of Internet of Things (IoT), a lot of healthcare data is being produced through the use of various devices like smart watches, smart sphygmomanometer, smart thermometer, etc. This imposes the need to concern about scalability along with interoperability. A novel architecture to handle the electronic medical records (EMR) of the patients by various medical entities is proposed. As large amounts of records are to be handled, the healthcare archives are kept in the cloud for streamlining the usage of information among diverse stakeholders. Also, there is a provision to enable the measures that handle security and privacy in the cloud architecture. Suitable public key cryptography and hashing methods are exploited to maintain the past transactions corresponding to the patients' records. This preserves confidentiality, integrity, and availability. It also prevents the modification or falsification of data by unauthorized persons. Using blockchains, patients' records can be added only at the end of the database, but they cannot be removed. New records are securely connected to the preceding record using cryptographic hashing. Special node called data validator is used to check the quality and authenticity of user-uploaded data, from which the records can be examined and patient health status

R. Ramya (✉) · A. Anandh · K. Muthulakshmi · S. Janani
Department of Computer Science and Engineering, Kamaraj College of Engineering and Technology, Madurai, Tamil Nadu, India
e-mail: ramyacse@kamarajengg.edu.in; anandhcse@kamarajengg.edu.in; muthulakshmicse@kamarajengg.edu.in; jananicse@kamarajengg.edu.in

N. Gayathri
School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
e-mail: n.gayathri@galgotiasuniversity.edu.in

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_9

reports are prepared. Again, encryption and digital signing are performed on the data to store it back to the blockchain. This proposed system ensures that no individual can modify or damage the verified records that are already stored. Our proposed novel architecture was tested against MIT-BIH Arrhythmia Database, and the stated functionality requirements are met.

Keywords Smart healthcare · Cryptography · Blockchain · Cloud · Validator · Security

1 Introduction

In recent years, vast sensors and devices are connected through the Internet for achieving various applications. The most essential part of our life, the medical care, results in an outstanding increase in the volume of medical data that is being generated. IoT-based wearable technology employed by healthcare professionals to streamline the medical diagnosis and curative process is the main reason behind this. These applications may cause privacy and security risks during data transfer and data log maintenance. These issues may endanger the life of the patient.

Using wireless body area networks (WBANs), Farrukh Aslam Khan et al. developed a remote and easily deployable healthcare system [8]. A key generation scheme based on multi-biometrics is used to secure the inter-sensor communication in WBANs. Moreover, patient details are securely maintained in the hospitals by storing the EMRs in cloud. This system suffers from the interference between different sensors that share the channel. The challenges related to performance, usability, and security of the system were not addressed.

Fine-grained access control and flexibility are lacking in traditional schemes of encryption, and hence they are not appropriate to provide access control in cloud [9, 16, 17]. In cloud, privacy and secure access are maintained using attribute-based encryption (ABE) [21]. Various ABE schemes have been introduced to enhance the productivity and security issues in cloud [27–31]. Pardeep Sharma et al. [26] brought out the challenging issues, deployment models, and key security problems that are currently faced by cloud computing. Different service models and its requirement of security were also discussed. After examining the threats in the cloud environment, the approach of blockchain technology to secure cloud data was focused by Hang Xu et al. [12]. To provide an authentic cloud virtualization environment for data, they proposed a blockchain-based cloud forensic storage architecture model.

The introduction of cloud computing in the healthcare industry creates many security and privacy issues for individuals and healthcare providers according to Yazan Al-Issa et al. [46]. They concluded that the safety, privacy, productivity, and extensibility concerns are obstructing the wide transformation of the cloud technology in healthcare, and hence the precautions like firewalls, intrusion detection, and

the type of encryption and authentication should be examined. Saleh et al. discussed about the healthcare cloud to store and secure information [36]. Furthermore, security issues in cloud computing, especially in the perspective of healthcare cloud, were introduced.

The concept beyond cryptocurrency that uses blockchain technology was discussed by Sharma et al. They also outlined the application and impact of cryptocurrency in big data [38]. A system that ensures authentication and provides integrity to health data was proposed by Nagasubramanian et al. Authentication was ensured by using keyless signature infrastructure, whereas integrity was ensured by the use of blockchain [24]. An IoT-based framework for analyzing pharmaceutical data was proposed by Dhingra et al. [6]. This system can be used to detect the early symptoms of chronic, long-term diseases.

Zibin Zheng et al. presented an overview about the architecture and key characteristics of blockchain [48]. They explored the typical consensus algorithm that is used in blockchain. The challenges faced by blockchain were also described. Sachchidanand Singh concentrated on the role of blockchain in shaping the banking services, financial institutions, and adoption of Internet of Things [34]. For delivering healthcare information facility, a cloud computing-based healthcare software-as-a-service (SaaS) platform (HSP) was developed by Sungyoung Oh et al. [40]. For cloud-based SaaS services, clinical decision support (CDS) content services and basic functional and mobile services were focused. Microsoft's Azure cloud computing was used for infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS).

Christian Esposito et al. in healthcare [5] observed that progressive transfer of data and services to the cloud is the trend nowadays. They pointed out that there are restrictions to use conventional cryptographic algorithms and access control models to address security and privacy concerns in cloud-based environment. Shan Jiang et al. proposed blockchain-based environment for healthcare information exchange [37]. Two loosely coupled blockchains were implemented to handle different types of healthcare data. Off-chain storage and on-chain verification were combined to assure the requirements of both privacy and authenticity. Moreover, two fairness-based packing algorithms were introduced to improve the system productivity and fairness among the users. Zainab Alhadhrami et al. proposed a permissioned and permissionless blockchain implemented for healthcare system [47]. Tareq Ahram et al. formalized and developed a healthcare industry application, using IBM blockchain initiative [42]. Matthias Mettler et al. suggested that blockchain has a massive potential for the future and will show attention-seeking changes in the healthcare industry [22].

Tran LE Nguyen et al. created a graphical, abstract model of medicinal application using blockchain technology to manage all information of patients and doctors after they have a surgery [43]. The model was engineered based on the hole of the previous models in banking and finance sectors that are using blockchain. A smartphone application using Bitcoin in payment was also developed for the doctors to manage their patients and to help the patients to have a good differentiation of cost about the procedure for the preparation of pre- and post-surgery. Vojislav B. Misic

et al. proposed a blockchain-based healthcare system architecture in which the block validation is done using the collective signatures of the leader and a pool of witnesses [45]. Moreover, they delineated a smart contract-based approach that permits knowledge to homeowners to expressly grant or revoke authorizations for other users to access healthcare data. All accesses are stored and maintained on the blockchain as separate transactions, in order to provide certain transparency and privacy protection.

Tanesh Kumar et al. highlighted the conception of smart contract for blockchain-based healthcare systems, which is the key to define the concurrence between various end users [41]. Leila Ismail et al. projected a lightweight blockchain design for the healthcare data maintenance that reduces the processing and overhead in communication as compared to the Bitcoin network. In Bitcoin network, the network was divided into clusters, and one copy of the ledger in each cluster was maintained [20]. The introduction of the canal permits stable and secret transactions with a network cluster. Different threats and attacks were also analyzed. Vidhya Ramani et al. projected an Ethereum-based implementation technique for secured data access mechanisms [44]. It guarantees that only the solely approved system can access the patients' medical information. This technique is resistant to known attacks and maintains the honesty of the system.

Although blockchains are used to begin the smart contracts between healthcare providers, there exists potential problem to identify whether the authorized person is accessing certain data or patients' records. Another major issue that could endanger the protected health information (PHI) and EMR is the implementation nature of blockchains. It does not ensure the confidentiality of the data which is stored or transported off chain. Sybil attack is an additional security issue. A single attacker or group of attackers are pretending as multiple nodes and gain control of the network. To ensure integrity, blockchains fully rely on a set of cryptographic algorithms. If quantum computers come into existence, the security and integrity of the whole network can be compromised. Quantum computers have greater processing speeds because of using qubits instead of binary bits. It allows the attacker to falsify blocks by recomputing the hash value of the blocks in a polynomial time. Blockchain technology and cloud computing-based approach were used to solve the interactivity and stability issues in basic healthcare system and to handle the voluminous of data. Once the healthcare data is stored, they can be analyzed using various features [2] that are extracted using machine learning algorithms [10, 19] or using deep learning framework [33].

2 Preliminaries

2.1 An Overview of Healthcare Systems

Nowadays, in many countries, healthcare has come into play. Healthcare system deals with the health needs of most population such as a group of people or institutions. It includes access to resources such as services, expenditures, healthcare workers, and facilities. Improving the fitness of people using society's existing assets and challenging needs is the main objective of this system. Patients, healthcare team, and community resource providers are the different groups in the healthcare system. These systems of nations must be designed and developed based on the needs and resource convenience. In all health systems, primary healthcare and public health measures are the common essentials. Some countries plan health system among market members.

Healthcare involves clinic systems, patient attention, insurance, healthcare providers, and the authorization problems in all these components. Hospitals, clinics, and community health agencies vary from other labor surroundings. These structures remain more composite, and persons used up to this structure must know all the terms.

Culture and past history are the factors that influence the range of a system to build a precise structure. With a nation's growth, culture, and societal ethics, this can vary markedly in accordance with healthcare. Gerdtham and Jonsson stated that the level of economic resources available has an effect on the healthcare system's structure. According to per capita gross domestic product (GDP), medical expenses, and the share of a nation's GDP, there is a strong positive correlation between economic resources spent on healthcare [11, 38].

Along with health promotion and disease prevention, healthcare structures involve worldwide access to complete prepaid healthcare. In the developed world, country's health insurance facilities of different replicas had evolved. Numbers of countries use models like Bismarckian social security and Bereidge National Health Service as pioneered in Canada. Except the United States, all industrialized countries have different worldwide structures of medical coverage involving collaborated public and private insurance. In spite of this, a high percentage of uninsured and poorly insured are available. Every nation wants to encourage medical care for all; medical improvement is a continuous procedure. Nations must adapt funding schemes for medical care, health safety, and advancement to elder peoples, cumulative costs, and equipment. The basic healthcare system contains several security issues to safely handle the data. So we look into the insights of healthcare system issues and discuss the solution to solve these issues.

2.2 An Overview of Security Issues in Healthcare Systems

One of the promising fields in wireless sensor networks is healthcare applications, in which the patients are supervised with wireless medical sensor networks (WMSN). It focuses on areas such as patient mobility, reliable communication, and efficient routing for energy efficiency for research. But, without security, the deployment of new technologies in medical application makes the patient's private information susceptible.

Kumar et al. [15] discussed that security is a significant prerequisite in medical applications as the health information of individuals are extremely sensitive, mainly if the patient has an embarrassing disease. The success of medical application mainly relies on the safety of patients because of legal and ethical reasons. WMSN are used to make the victims' existence more relaxed. They give viable answers in various healthcare applications. The success of any wireless medical application relies on security measures used. Using WMSN is an evolving research area, which is a valuable learning for achieving security.

Our daily life depends heavily on smart devices that fall under the category of IoT gadgets. These gadgets become a part and parcel of our lifestyle, with healthcare becoming the crucial area. Healthcare can also be made easy using fog computing that makes the information transfer possible through IoT devices. The major issues raised by them are interoperability and security. Karthika et al. discussed about the various issues and ways to deal with those issues to avoid them by utilizing the gadgets available in medicinal services framework [13]. Fog computing focused mainly on monitoring the patients with continuous illness. By sharing the executing modules among the applications belonging to the same healthcare solutions, computational load can be made optimal. Moreover, the recently deployed modules of terminated applications can be reused for other applications also. For this purpose, necessary techniques must be developed.

Wireless sensor networks (WSN) are evolving over time because of the sensors that are of low cost and short range and are easy to deploy. WSN senses and transmits the real time information of the specific environment that is monitored for further processing and examination. Security and privacy in WSNs are becoming an important research area due to the popularity of wireless channels [18, 35]. A brief introduction about cloud computing and blockchain technology is discussed in the following section for the sake of users to recollect.

2.3 An Overview of Cloud Computing

As an individual, a person stores programs and data in a hard disk. Programs and data get accessed whenever it is needed. This process is termed as "computing." Now, because of technology advancement, the need for storing in our physical hard disk keeps vanishing. Here comes cloud computing into the picture. It is a method

of computing in which the programs and data are stored on cloud over the Internet. In case of an organization, requirements are increasing day by day. The requirements are not only restricted to storage. It can also be a server, application, infrastructure, etc. Creating requirements from scratch may be a time-consuming and expensive task. So, this brings the culture of "pay on use", i.e., the users of the cloud will get a share of already available resources over the cloud.

Cloud computing is an alternate way to the method of managing on-premise data center. Here, the cloud vendor has to take care of everything from purchase and installation of hardware, OS and needed application installation, virtualization, network and firewall configuration, and, finally, maintenance of all of these throughout their life. They provide a different variety of software, infrastructure, and platform as a service. So, here the users rent the services depending on their need, and the users will be charged based on the usage.

Many cloud providers, such as Microsoft Azure, VMware, Amazon Web Services, Google cloud platform, etc., are available. They make the management of resources such as compute, storage, network, and applications handy.

It reduces the initial investment to buy the hardware as well as software. There is no need for the maintenance also, leading to less operational efforts. Within few clicks, the resources can be accessed with ease. Services are highly reliable, and according to our requirements, resources are scalable, providing rapid elasticity. Users need to pay only for what resources they use. It also provides data security using a variety of policies and technologies. The resources are available round the clock, and based on demand, it can be used dynamically and automatically. There is no restriction on the mode in which resources are accessed, i.e., the clients can be homogeneous/heterogeneous, thin or thick [1, 3].

2.4 An Overview of Blockchain Technology

In this digital era, increasing industrial growth needs trusted customer relationship. Blockchain, the foundation of cryptocurrency, is a distributed ledger that provides an authenticated way of exchanging information in terms of transaction. The intriguing features of blockchain technology pave a way to receive extensive attention globally in various sectors including business and commercial services. As a decentralized ledger, it stores a list of transactions which are propagating constantly, and its replicas are distributed among the members of a network. The two key features of blockchain, namely, immutability and non-repudiability, are vital to support applications which require faster product innovations, trusted partnerships, and fast integration with the mass storage technology such as cloud technology and IoT. The immutability is defined as impossibility of committed transaction modification in the blockchain. Non-repudiation is also achieved by having the identity of transaction involved by large number of entities. Traditionally, database access is controlled by centralized authentication system. Subsequently, limited right credentials and limited capacity of the system tend to make the database access difficult. As a

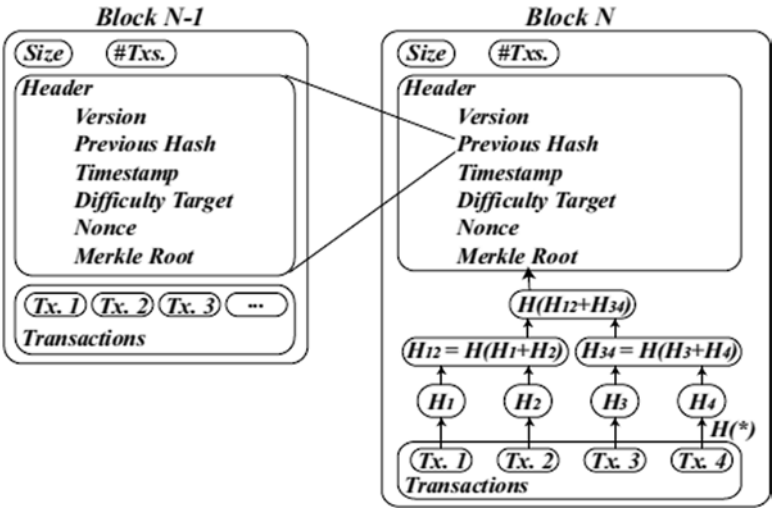


Fig. 1 Structure of traditional blockchain

distributed ledger, blockchain addresses the challenges in accessing the database. Here, the individual transactions are converted into encoded blocks by exploiting the relevant encryption techniques, added to the ledger, and never removed. The data in the blockchain is secured by hash technique. For any input data, hash value is created by encryption of input data using hash function.

Structure of traditional blockchain is depicted in Fig. 1. The significant components of a single block are the size of the block, transaction counter, block header, and transaction details. The block size is represented in bytes. The number of transactions is termed as transaction counter. The block header includes version number, hash value of the previous block, time of creation, target, padding bits, and Merkle root. Consensus protocol updates can be tracked by verifying the version number. Timestamp value represents creation time of the block, and the padding bits are maintained for enabling proof-of-work consensus protocol. The Merkle root indicates the hash value of all the hashes that are created for the entire transactions. The hash value of the previous block is also associated with the chain. Block header is hashed twice using SHA-256 hash function, and the value of hash is stored as the primary identifier of a block [4, 23].

Blockchain techniques are categorized into permissionless and permissioned blockchains. In permissionless blockchains, otherwise known as public blockchains, there is no need to rely on the third party for participating in the network and performing transactions. Blockchain enables the validation, storing, and maintaining of transaction records which are done in the network, and the node access is made public. Regarding security, vulnerability is resolved by maintaining the replicas in other nodes in a distributed manner. As opposed to permissionless blockchains, permissioned blockchains are introduced to avoid public accessibility. For storing and transmitting sensitive information like healthcare records, it is enforced

to provide confidentiality, privacy, and better scalability. Permissioned blockchains are further categorized into private and consortium blockchains. In private blockchains, write permissions are restricted to centralized authority only, and read permissions are made public or restricted to an extent. While in consortium blockchains, the operations are regulated by a predefined set of trusted nodes through consensus process.

Blockchain technology is mainly employed in financial and banking sectors. Due to its pertinent characteristics such as decentralization and immutability, it becomes a powerful tool in healthcare sector, too. It creates an extensive range of breakthroughs in healthcare systems and defines predefined contracts among the various stakeholders. It provides a secure way to share the data between information providers, patients, and agencies involved in healthcare systems. It leads the researchers to focus and to explore the significant methodologies for blockchain-powered healthcare.

3 Proposed Blockchain-Powered Healthcare System

Blockchain can play a vital part in the renovation and digitization of industries by tight integration with technologies such as cloud computing and IoT. One of the secure ways to exchange several types of information is blockchain. Earlier, a reliable third party is mandatory to make settlement about services. With the use of blockchain, transactions can be made, directly eliminating the need for central entity controlling the data. This feature in blockchain technology strongly affects the behavior of existing healthcare market players. Blockchain also provided the way to promote new models and initiatives in business. Intermediaries (data) are avoided by using this blockchain technology [25]. It paves a new way with respect to how a market interaction in healthcare is conducted.

3.1 Proposed System Overview

A novel architecture for managing and sharing EMR of patients by various medical entities is proposed. As large amount of records are to be handled, the healthcare archives are kept in the cloud for streamlining the usage of information among the diverse stakeholders. Also, there is a provision to enable measures to handle security and privacy in the cloud architecture. Figure 2 shows the novel architecture of blockchain-powered healthcare system.

The proposed architecture consists of blockchain and cloud storage to facilitate data storage. Medical data of small size like patient medical history and prescription details are stored in blockchain. Volumetric medical data of large size, such as scan images, EEG/ECG records, etc., are stored in cloud in encrypted format, and the details of access rights and owner information are recorded in blockchain. Any

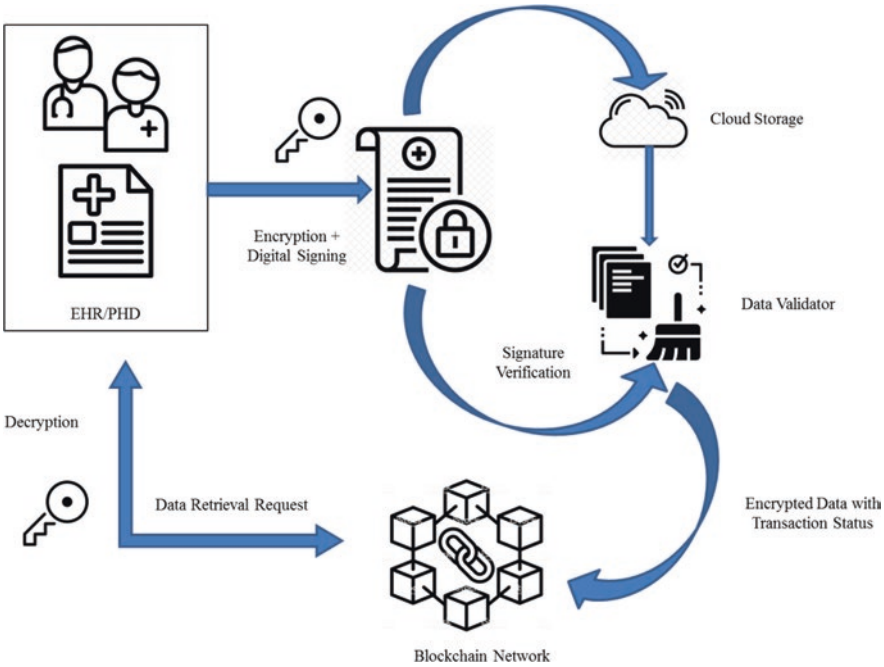


Fig. 2 Blockchain-powered healthcare system

company that meets the protocols of Health Insurance Portability and Accountability Act (HIPPA) can act as the cloud storage provider. Here, we used Amazon Web Services (AWS) for the experimentation purpose.

3.2 Notations Used in the Proposed System

Table 1 shows the notations that are used in our proposed system architecture for managing and sharing EMR of patients by various medical entities.

3.3 Three Major Entities in Our Proposed Architecture

The three major entities present in the proposed architecture are:

1. Blockchain network – To store and share the collected medical data. This includes network clusters, data validators, and authentication generator. Whenever the data is uploaded, network participant will decide whether to record the data in blockchain network or not. Data validators are responsible for validat-

Table 1 Notations used

Notation	Description
D	Doctor
U	User/Patient
idU, idD	ID of patient and doctor
pubU, pubD	Public key of patient and doctor
privU, privD	Private key of patient and doctor
kUD	Secret key shareable between patient and doctor
E(.), D(.)	Encryption/Decryption function
H(.)	Hash function
D	Patient data
RK	Registration kernel
RKc	Certificate by registration kernel
reqM	Request message
Vd	Voluminous data
T	Timestamp
C	Consent detail: yes/no

ing the quality and authenticity of medical data. Authentication generator makes the data anonymized by removing the patient ID and creates electronic signature of data

2. Patient/Users – Individuals who are ready to share the data. Data are being generated from IoT devices in smart home environment, the personal healthcare data (PHD) or in hospitals during diagnosis, and the electronic medical record (EMR).
3. Medical institutions/Research centers – Can access anonymized data for treatment or research purpose.

3.4 Three Major Phases of Our Proposed Architecture

The three major phases of blockchain-powered healthcare architecture are as follows:

(i) *Data Registration* – The user/patient must register their personal, identifiable details in the registration kernel (RK) before their medical data is uploaded into the blockchain network. The steps involved for registration are shown in Algorithm 1.

(ii) *Data Addition/Update* – The steps involved in adding PHD and/or EMR are mentioned in Algorithm 2.

(iii) *Data Retrieval from Blockchain* – The steps involved for retrieving data from blockchain are mentioned in Algorithm 3.

Algorithm 1 Data Registration

(a) For every user/patient record, a unique id (idU), the public key of patient (pubU), and the public key of doctor (pubD) are generated.
(b) RK sends these details to the blockchain along with its digital signature and patient's digital signature.
(c) SHA-256 algorithm is used to generate hash value which forms the digital signature.
(d) If the details are stored for the first time, blockchain confirms the digital signatures of both the patient and RK, and then, it stores idU, idD, pubU, and pubD on the network.

Algorithm 2 Data Addition/Update

(a) To add or update the EMR (the details such as patient ID, treatment details, medical history, and billing information), the doctor encrypts the data, D, by using the symmetric key, kUD, shareable with the patient after getting approval from patient and generates encrypted data E(D).
(b) The doctor creates his own digital signature H(privD,T1) with timestamp T1 and sends the encrypted data E(idD||H(privD,T1) || E(D) || pubD, kUD) to the patient for verification.
(c) The patient decrypts and verifies the doctor details and creates his/her own digital signature H(PrivU,T2) with timestamp T2 and sends back the encrypted data E(idU||H(PrivU,T2) || E(D) || pubU || C, kUD) to the doctor. C indicates the consent of the patient to add the data to the blockchain or not.
(d) The doctor checks the data sent by the patient for consistency. If the check returns true, E(idD || idU || E(D) || pubD || T3 || RKc, privD) data is directed to the blockchain for further processing.
(e) When the blockchain gets notified for addition/update, the data validator verifies the timestamp, RKc, and authenticity of the doctor at the blockchain end. If it is positive, then the details are added/updated in the ledger, and the copy of T4 || idD || pubD along with transaction status, Txn, is transmitted to other participants in the network. Patients can also store PHD in the network, encrypted by their private key, privU, after following the above verification steps.
(f) To store the voluminous data such as scanned images or EEG/ECG details, the ID of the patient is eliminated from the data for anonymity, and the data Vd || pubD is stored in the cloud storage by following the above steps.

Algorithm 3 Data Retrieval

(a) If a doctor tries to assess data from the blockchain in a particular time frame, request message, reqM = IdD || H(privD, T) || idU is generated and sent to the blockchain network.
(b) Then, these details are verified at the blockchain network end.
(c) Once the verification is done, the data of the corresponding patient is identified using idD and published to the doctor.

Suitable public key cryptography and hashing methods are exploited to maintain the past transactions that correspond to patients' records. This preserves the confidentiality, integrity, and availability [7]. Hence, this architecture ensures that no individual can alter or damage the verified records that are already stored, preventing the modification or falsification of data by unauthorized users. In blockchains, new records can be securely connected to the preceding record using cryptographic hashing. Special node, data validator, is used to check the quality and authenticity of user-uploaded data. In addition to that, blockchains are also used to afford customized, encrypted health recommendations to patients without the necessity to disclose their identities.

3.5 Security Measures

Lightweight data communication is achieved by clustering the blockchain nodes and storing the data in one node, i.e., a single copy of the data is maintained per cluster. However, the transaction status is maintained in all the nodes as a backup to address any unavoidable crashes [14, 39].

For symmetric encryption, Advanced Encryption Standard (AES) algorithm is used in the proposed system to provide confidentiality since the patient information is sensitive to alteration by unauthorized ones. Elliptic curve cryptography is used for public key encryption which preserves authenticity of the doctor and patient and for providing lightweight data communication. Digital signature is derived by exploiting SHA-256 algorithm. We take the advantage of timestamp and digital signature to maintain the integrity of the message [32].

4 Results and Discussion

4.1 Experimental Results

Experimentations were performed using a Dell Core i7 processor 3.2 GHz PC that has 6GB of RAM. Our proposed novel architecture is tested against MIT-BIH Arrhythmia Database. Figures 3 and 4 show the comparison of data that are transferred in MB and processing time required for updating the ledger using our proposed architecture with the other state-of-the-art approaches [15]. From these, we can infer that our proposed system performs better as compared to other approaches.

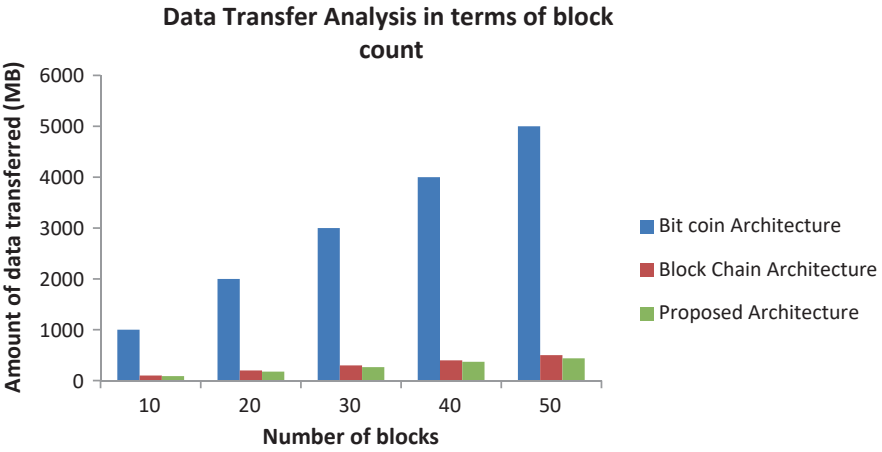


Fig. 3 Data transfer analysis in terms of block count

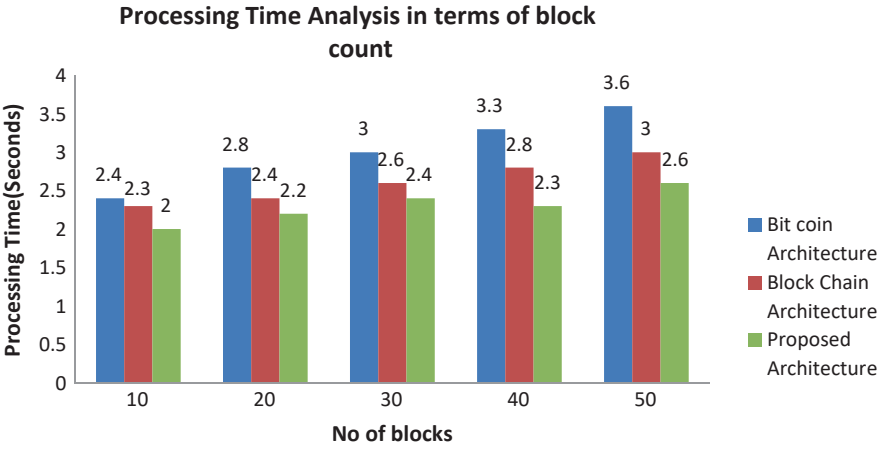


Fig. 4 Processing time analysis in terms of block count

4.2 Discussion

In our proposed method, each patient's health record information is encrypted using symmetric encryption technique. Transactions between the patients and doctors, who are in the network, are performed by using AES encryption and decryption process.

Researchers and doctors are the external users who may access these health records. Elliptic curve cryptographic algorithm is used for this public decryption process. The order of the group G is chosen as 160-bit. The large prime P is of

512-bit that is used to build pairing from an elliptic curve. Even though it is time-consuming, it ensures high security in terms of confidentiality.

Registration kernel ensures authenticity. Similar to existing blockchain networks, our proposed system uses blocks to keep track of the past transactions. Here, each block holds a hash value. To provide digital signature, SHA-256 is chosen because of its fame in the Bitcoin network. In existing frameworks, irrelevant of size, the entire data of patient is stored in blockchain only. But in the proposed system, voluminous data is stored in cloud storage. Using our system, the time taken to transfer the data gets reduced. Reliability is also not compromised as in the existing frameworks because the information about the data is maintained in all the ledgers and it ensures that there is no possibility to lose the data.

5 Conclusion

Various technologies are emerging at a rapid rate with technological advancements. They have the capability to make human's lives easier. To use these technologies, one must be very careful to realize the security risks posed as well as the limitations. Security, particularly privacy, is a predominant demand in healthcare domain when the patients turn out with embarrassing malady. For providing such a secured management of healthcare data and to make the health services more affordable, blockchain-based system architecture is proposed. Though blockchains need intensive computations, demanding more bandwidth and extra power, they are more suitable for our environment which is not constrained toward resources. Our proposed novel architecture is tested against MIT-BIH Arrhythmia Database, and the stated functionality requirements are met.

References

1. M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: opportunities and challenges. Inf. Sci. **305**, 357–383 (2015)
2. A. Anandh, K. Mala, R. Suresh Babu, Combined global and local semantic feature–based image retrieval analysis with interactive feedback. Meas. Control **53**(1–2), 3–17 (2020). https://doi.org/10.1177/0020294018824122
3. M. Barua, R. Lu, X. Shen, SPS: Secure personal health information sharing with patient-centric access control in cloud computing, in *2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA*, (IEEE, 2013), pp. 647–652
4. R. Chandran, S.R. Kumar, N. Gayathri, Genetic algorithm-based tabu search for optimal energy-aware allocation of data center resources. Soft. Comput. **24**(21), 16705–16718 (2020). https://doi.org/10.1007/s00500-020-05240-9
5. C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K.R. Choo, Blockchain: a panacea for healthcare cloud-based data security and privacy. IEEE Cloud Comput. **5**(1), 31–37 (2018)

6. P. Dhingra, N. Gayathri, S.R. Kumar, V. Singanamalla, C. Ramesh, B. Balamurugan, Internet of Things–based pharmaceutics data analysis, in *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*, (Academic Press, London, 2020), pp. 85–131
7. A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**, 326 (2019)
8. F.A. Khan, A. Ali, H. Abbas, N.A.H. Haldar, A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. The 2nd International Workshop on Communications and Sensor Networks. Procedia Comput. Sci. **34**, 511–517 (2014)
9. M.S. Ferdous, A. Margheri, F. Paci, M. Yang, V. Sassone, Decentralised runtime monitoring for access control systems in cloud federations, in *IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, (IEEE, 2017), pp. 2632–2633
10. G. Nagasubramanian, M. Sankayya, F. Al-Turjman, G. Tsaramirsis, Parkinson data analysis and prediction system using multi-variant stacked auto encoder. IEEE Access **8**, 127004–127013 (2020). https://doi.org/10.1109/ACCESS.2020.3007140
11. U.-G. Gerdtham, B. Jonsson, International comparisons of health expenditure: theory, data and econometric analysis, in *Handbook of Health Economics*, ed. by A. J. Culyer, J. P. Newhouse, vol. 1, 1st edn., (Elsevier, 2000), pp. 11–53
12. H. Xu, J. Cao, J. Zhang, L. Gong, Z. Gu, A survey: cloud data security based on blockchain technology, in *IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, (IEEE, 2019), pp. 618–624
13. P. Karthika, R. Ganesh Babu, P.A. Karthik, Fog computing using interoperability and IoT security issues in health care, in *Micro-Electronics and Telecommunication Engineering*, (Springer, Singapore, 2020), pp. 97–105
14. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, Boca Raton, 2020)
15. P. Kumar, H.-J. Lee, Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors **12**, 55–91 (2012)
16. P.P. Kumar, P.S. Kumar, P.J.A. Alphonse, An efficient ciphertext policy-attribute based encryption for big data access control in cloud computing, in *2017 Ninth International Conference on Advanced Computing (ICoAC)*, (IEEE, 2017), pp. 114–120
17. P.P. Kumar, P. Syam Kumar, P.J.A. Alphonse, Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. J. Netw. Comput. Appl. **108**, 37–52 (2018)
18. S.R. Kumar, N. Gayathri, Trust based data transmission mechanism in manet using solsr, in *Annual Convention of the Computer Society of India*, (Springer, Singapore, 2016), pp. 169–180
19. S.R. Kumar, N. Gayathri, S. Muthuramalingam, B. Balamurugan, C. Ramesh, M.K. Nallakaruppan, Medical big data mining and processing in E-healthcare, in *Internet of Things in Biomedical Engineering*, (Academic Press, Amsterdam, 2019), pp. 323–339
20. L. Ismail, H. Materwala, S. Zeadally, Lightweight blockchain for healthcare. IEEE Access **7**, 149936–149951 (2019)
21. M. Li, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. **8**(3), 2084–2123 (2016)
22. M. Mettler, Blockchain technology in healthcare: the revolution starts here, in *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, (IEEE, 2016), pp. 1–8, 978-1-5090-3370-6.
23. G. Nagasubramanian, M. Sankayya, Multi-variate vocal data analysis for detection of Parkinson disease using deep learning. Neural Comput. & Applic. **64**, 1–16 (2020)
24. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
25. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, *Blockchain Databases. Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, Boca Raton, 2020)
26. P. Sharma, S.K. Sood, S. Kaur, Security issues in cloud computing A. Mantri et al. (ed.) HPAGC 2011, CCIS 169, pp. 36–45 (2011)

27. P.K. Premkamal, S.K. Pasupuleti, P.J.A. Alphonse, A new verifiable outsourced ciphertext-policy attribute based encryption for big data privacy and access control in cloud. J. Ambient Intell. Hum. Comput. **10**(7), 2693–2707 (2019)
28. P.K. Premkamal, S.K. Pasupuleti, P.J.A. Alphonse, Dynamic traceable CP-ABE with revocation for outsourced big data in cloud storage. Int. J. Commun. Syst. **34**(2), e4351 (2020)
29. P.K. Premkamal, S.K. Pasupuleti, P.J.A. Alphonse, Efficient revocable CP-ABE for big data access control in cloud computing. Int. J. Secur. Netw. **14**(3), 119–132 (2019)
30. P.K. Premkamal, S.K. Pasupuleti, P.J.A. Alphonse, Traceable CP-ABE for outsourced big data in cloud storage, in *International Conference on Computing and Information Technology*, (Springer, Cham, 2019), pp. 213–226
31. P.K. Premkamal, S.K. Pasupuleti, P.J.A. Alphonse, Efficient escrow-free CP-ABE with constant size ciphertext and secret key for big data storage in cloud. Int. J Cloud Appl. Comput. **10**(1), 28–45 (2020)
32. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, Boca Raton, 2020), pp. 1–23
33. R. Ramya, K. Mala, S. Selva Nidhyananthan, 3D facial expression recognition using multi-channel deep learning framework. Circuits Syst. Signal Process. **39**, 789–804 (2020). https://doi.org/10.1007/s00034-019-01144-8
34. S. Singh, Blockchain: future of financial and cyber security. Contemp. Comput. Inf. **2**, 463–466 (2016)
35. R.K. Sakthivel, G. Nagasubramanian, F. Al-Turjman, M. Sankayya, Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. Trans. Emerging Telecommun. Technol. **2020**, e3947 (2020). https://doi.org/10.1002/ett.3947
36. S.M. Altowaijri, An architecture to improve the security of cloud computing in the healthcare sector, in *Smart Infrastructure and Applications*, (Springer, Cham, 2020), pp. 249–266
37. S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, J. He, BlocHIE: a blockchain-based platform for healthcare information exchange. IEEE Smart Comput. **43**, 49–56 (2018)
38. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195
39. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global, 2021), pp. 165–177
40. O. Sungyoung, J. Cha, M. Ji, H. Kang, S. Kim, E. Heo, J.S. Han, H. Kang, H. Chae, H. Hwang, S. Yoo, Architecture design of healthcare software-as-a-service platform for cloud-based clinical decision support service. Health Inf. Res. **21**(2), 102–110 (2015)
41. T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila, Blockchain utilization in healthcare: key requirements and challenges, in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, (IEEE, 2018), pp. 1–7, 978-1-5386-4294-8.
42. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, Blockchain technology innovations, in *2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, (IEEE, 2017), pp. 137–141, 978-1-5090-1114-8.
43. T. Le Nguyen, Blockchain in healthcare: a new technology benefit for both patients and doctors, in *2018 Portland International Conference on Management of Engineering and Technology (PICMET)*, (IEEE, 2018), pp. 1–6, 978-1-890843-37-3.
44. V. Ramani, T. Kumar, A. Bracken, M. Liyanage, M. Ylianttila, Secure and efficient data accessibility in blockchain based healthcare systems, in *2018 IEEE Global Communications Conference (GLOBECOM)*, (IEEE, 2018), pp. 206–212, 978-1-5386-4727-1.
45. V.B. Mišić, J. Mišić, X. Chang, Towards a blockchain-based healthcare information system, in *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, (IEEE, 2019), pp. 13–17

46. Y. Al-Issa, M.A. Ottom, A. Tamrawi, eHealth cloud security challenges: a survey. Hindawi J. Healthcare Eng. **2019**, 1–15 (2019)
47. Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J.A. Abedlla, K. Shuaib, Introducing blockchains for healthcare, in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, (IEEE, 2017), pp. 1–4, 978-1-5386-0872-2.
48. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends. IEEE Congress Big Data **6**, 557–564 (2017)

The Future of Cloud Computing: Blockchain-Based Decentralized Cloud/Fog Solutions – Challenges, Opportunities, and Standards

N. Krishnaraj, Kiranmai Bellam, B. Sivakumar, and A. Daniel

Abstract By allowing the creation of fully decentralized cloud/fog technologies that reduce costs by producing predictable outcomes without needing any intermediary, smart contracts and blockchain have had the opportunity to alter the present shape of cloud markets. In addition, many recommend current requirements for the creation of fully integrated decentralized cloud solutions that would allow large vendors to comply with these kinds of solutions and avoid proprietary hardware. We claim that certain analysis contributes to the advancement of cloud systems not only by figuring out implementation incompatibilities and alternative solutions to development issues in the field but also through evaluating predetermined rules and proposing great possibilities for interoperability.

Keywords Cloud computing · Fog computing · Blockchain · Distributed ledgers · Smart contracts · Standards

N. Krishnaraj (✉) · B. Sivakumar
SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu, India
e-mail: krishnan2@srmist.edu.in; sivakumb2@srmist.edu.in

K. Bellam
Department of Computer Science, Prairie View A & M University, Prairie View, TX, USA
e-mail: kibellam@pvamu.edu

A. Daniel
School of Computing Science and Engineering, Galgotias University,
Greater Noida, UP, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_10

1 Introduction

Blockchain technology is indeed an online blockchain technique that enables a business with knowledge and lets it securely record its transactions. The ledger becomes encrypted, so contact between some of the organization and the peer-to-peer network can only really be achieved when something is checked in this field. Blockchain seems to be the easiest way to move information from A to B without thinking about the accumulated incorrect information in the ledger, since this would invalidate millions and examples of the entire chain. This framework ensures transparency, as the transactions that are reported are only checked by several parties, and no transaction in the ledger can be reversed at a later point by the party candidates. The technology behind the decentralized blockchain Bitcoin, created by a person known as Satoshi Nakamoto in 2008, is also known as blockchain. In a nutshell, built on a peer-to-peer network, the blockchain is briefly clarified as a transparent, trusted, and decentralized ledger. The whole new technology has also been a hot topic for researchers recently and has been promoted beyond Bitcoin to innovate blockchain-based applications. Decentralization is the main concept of the blockchain network, which suggests the blockchain is distributed over a node network. Each node has the ability to verify the behavior of other network entities, as well as the ability to make, authenticate, and validate the new transaction that is to be registered in the blockchain. With the benefits of tamper resistance and no single-point failure vulnerabilities, this decentralized architecture guarantees stable and safe blockchain operations [1, 2].

Some main components, including data block, distributed ledger, consensus, and smart contracts, are constructed from a blockchain network. To be transparent, each block contains a number of transactions and is connected via a hash label to its immediately previous block. In this way, it is possible to trace all blocks in the chain back to the previous one., and no alteration or alternation to block information is possible. A distributed ledger is a kind of database that is shared and replicated between peer-to-peer network entities. In addition, blockchain consensus is a mechanism used to reach agreement among multiple insecure nodes on a single data block, helping to ensure security in a blockchain network (Fig. 1). Finally, smart contracts are programmable systems that function on a blockchain network in compliance with predefined contractual conditions such as terms of payment, liens, confidentiality, and even regulation. The parties involved in the transaction validate each transaction. These transactions are often referred to as “blocks.” After each party verifies the transaction, the transaction involved is solved by a mathematical puzzle and inserted into the ledger chain. No other person may make an adjustment to the entry until any entry in the transaction is made. This makes it secure and genuine for the transaction. Originally designed for digital currencies such as Bitcoin, blockchain is now used to distribute digital knowledge (not for copying the technology).

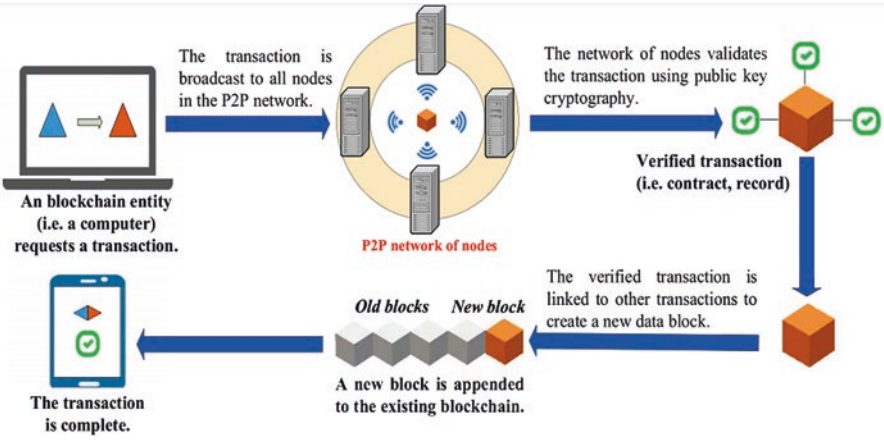


Fig. 1 Block transaction methods in node variables

Blockchain origins: Blockchain technology is a sort of distributed architecture that uses signed transactions that are cryptographic. It functions in a blockwise manner. Cryptographic systems are connected to each block [2, 3]. The validity of the transactions at each single point of failure should be validated and evaluated. It uses some peer-to-peer (P2P) model characteristics. The broker fees for approving the transactions are not incurred by this model (Fig. 2). Because this blockchain process provides its end systems with robust and scalable protection, blockchain technology is inclined to develop. Hackers also find it hard to hack the transaction systems' vulnerabilities. The transactions are, therefore, simpler and open to access. The basic components of the blockchain P2P architecture are presented.

Hashes: One of the key components of the blockchain model that adopts multiple use cases is hashes. The primary task is to encrypt the blocked information provided. Any size of data is computed. Changes made in the input can be seen in the output with the changes defined. For several real-time applications, the SHA-256 algorithm is extensively used [4, 5].

2 Open Chain Access Protocol

An abstract layer for accessing underlying blockchains is given by our open-source protocol. Our Open Chain Access Protocol allows the application to operate on multiple blockchains, similar to an ODBC or JDBC interface to a collection of databases. Chain connectors can be created by the group and encouraged by the reward process. And there is no need to modify the business logic or work with multiple chain technologies. This will allow more blockchain protocols to be supported and begin to progress [6].

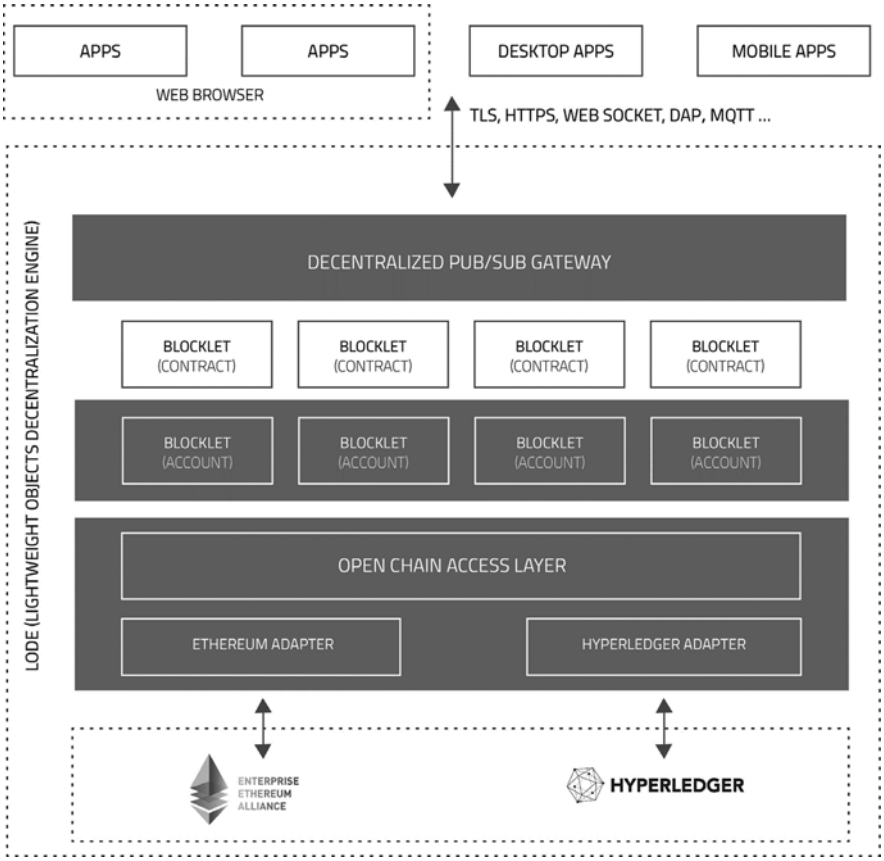


Fig. 2 Layer representation of blockchain

2.1 Blocklet

For executing different types of applications, blocklet is a part of the serverless computing architecture. For intelligent contracts, oracles, resource and asset handling, and off-chain business logic, use blocklet. By means of the Open Chain Access Protocol, blocklet interacts with blockchains and can be coordinated with our Algorand-based consensus algorithm. Anyone can use blocklet to create and contribute services and components under the incentive scheme. Group participants will earn tokens when their donations are used by others [7].

2.2 Components of Blocklet

Blocklet components are prebuilt blocklets that shape ArcBlock platform's base. Most of the features of ArcBlock are introduced with them (such as its token services, user identification services, etc.). Blocklet modules are incredibly customizable and interchangeable.

To get back up and running, integrate our prebuilt blocklet components into your applications. We include user information management elements, utility tokens, wallets, messaging systems for notification, and more. Use these out of the box or as flexible starting points for your own designs. The group may also build and donate blocklet element [8].

2.3 Computing with Services in the Cloud

Instead of a local server or a personal computer, cloud computing offers computing resources such as storage, databases, networking, and data processing over the Internet. It is often referred to as the "cloud." Here the cloud serves as an Internet metaphor. The cloud services you use are cost-effective, and the cloud computing scheme is used by major banks around the world to solve their data processing problems [9].

2.4 Ledgers

This consists of the transaction collection. Each node has transaction copies, i.e., ledger. In traditional model, pen and paper are commonly used for maintaining the ledgers. With the help of computer technology, the same principle has been applied and thus centralized.

The ledger is used with certain demerits, such as a single failure point, i.e., sudden loss of data and centralized committed transaction checks with a third-party agent [10].

2.5 Blocks

A transaction ID provided by end users is received by each node in blocks. The additional operations are carried out with this transaction index before the process ends. In the transactional phase, the mid-ops will not be saved. A transaction pool, the queue for all committed transactions, is maintained. At any step, mining nodes

are responsible for updating the transaction process. Therefore, a block is composed of a complete transaction collection, including the non-valid transactions[11].

The blockchain mechanism rejects transactions. This method confirms the rigidity of the data, as a change in a single bit of the block will drastically change the created hash. In addition, in order to improve protection, a copy of the hash of every block is shared among all the nodes. Because any node can check whether the hash matches, this method prevents any changes [12].

2.6 Cloud of Things

Nowadays, thanks to its great potential to offer exciting services across diverse applications, IoT has become a fundamental part of the future Internet and has gained growing interest from academics and industries. Heterogeneous devices and objects are seamlessly integrated by IoT to create a physical environment where sensing, processing, and communication processes are automatically applied without human intervention. However, because of the limited power and storage resources of IoT devices, vast amounts of data generated from a large number of devices in current IoT systems are a bottleneck in ensuring the desired quality of service (QoS). Meanwhile in terms of storage and processing capacity, cloud computing has infinite resources that can provide IoT realms with on-demand, effective, and efficient services. The integration of cloud computing with IoT, in particular, paves the way for a new paradigm like CoT that can empower both worlds. Indeed, IoT systems benefit tremendously from the abundance of resources available on the cloud, while the cloud can gain more prominence in real-life applications by integrating with IoT platforms. In addition, with minimal management effort, high system efficiency, and service availability, CoT can transform current IoT service provision models. IoT sensors are used to feel and gather data from local environments in this hierarchy. However, IoT devices can send recorded data to the cloud for data acquisition due to their limited computing resources. A strong data processing capability can be supported by cloud computing [13].

3 Cloud Computing Works

A computer dashboard is supported by cloud computing services, making it easier for IT professionals and developers to coordinate their manpower and efficiently manage business accounts. Actually, cloud services are developed to function with command line interfaces and REST APIs. Cloud computing operates on a conventional database architecture in which all the participants involved store the data on the servers. Restrictions, cross-compatibility difficulty, availability of services, and comparable costs can be obstacles on the flip side (Fig. 3). Although companies can breathe a little easier by removing licenses and the in-house configurations'

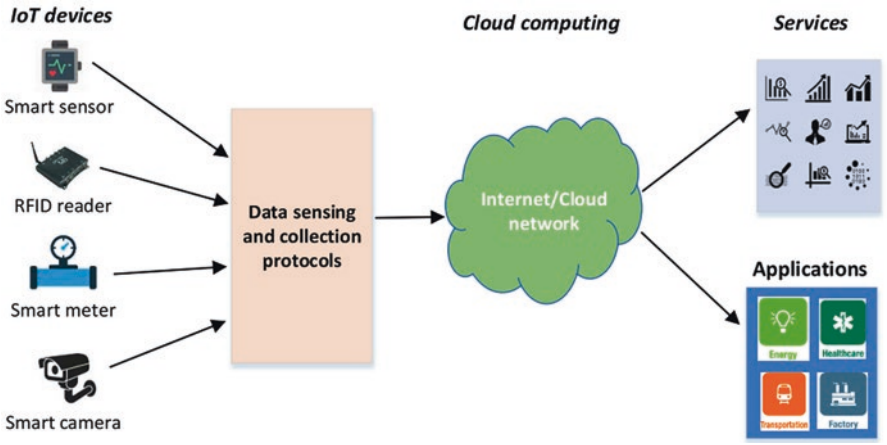


Fig. 3 Various devices connecting with blockchain model

portability issues, some problems still need to be addressed. For now, a widely available application for web or mobile apps, IoT, cloud-based BI data insights, and automated cloud services appears to be serverless. A transformative method to computing is demonstrated by the complete dependency on third-party hosts and microservices running with ready-made code. As the word suggests, the ultimate aim of server less is to remove the activity from on-premise to hosted facilities such as the cloud and substitute bundled functions for backend operations. Serverless seems to be able to improve "real-time testing" in a short time [14].

4 Blockchain's Best Features for Corporations

Blockchain is an incorruptible online economic transaction ledger that can only be programmed by validation from any participating party. Data is handled by a cluster of computers which are not controlled by a single entity, so that the information submitted is not corruptible [15].

In addition, because blockchain has broker-free functionality, there are no excessive fees that the parties involved in the transaction incur. When handling the blockchain transaction, companies incur no transaction costs other than paying for the technology architecture, so it can be a more cost-effective option for corporations than cloud computing [16].

Blockchain is able to disrupt many sectors, as it can be used not only to store financial transactions but also to manage the company's intellectual property and produce smart IP.

Blockchain attracts many industries for its possible applications in a technology-heavy world, as many kinds of information can be applied to the blockchain, ranging from blockchain networks to any sort of contractual information [17].

With blockchain, it is possible to store information about any or all of the intellectual property recorded, as well as any trademarks, designs, or patents that are still at the stage of registration or in the event of a dispute between the parties.

As the information stored cannot be changed, it can be used in any of the cases of trademark infringement or patent infringement faced by the proprietor after registration.

The IP register would also promote and establish an immutable record of events for the entire life of the intellectual property if registries start using the method. In the administration of patent registration and during patent evaluation, this can be extremely helpful [18, 19].

4.1 Risks and Benefits of Going Serverless

Serverless computing's most obvious threats include the inability to manage the client-side computing infrastructure, thereby restricting the reach of authoring tools. Additional limitations can be implemented by the cloud service provider (CSP) that circumvents the applicability of particular use cases. Further security issues can involve public clouds dealing with many customers (Fig. 4).

As the consumer does not perform checks on hosted services directly, enforcement can be a major concern. Certain organizations can also prefer a server-based architecture for proprietary studies.

It can be a hassle and time-consuming effort if a customer needs a CSP switchover.

Unique tasks can include other applications from third parties, raising the overall cost of a CSP's provision of services.

As early as 2008, several common FaaS services were in use such as AWS Lambda and MS Azure. For serverless, this was an obvious issue as too many

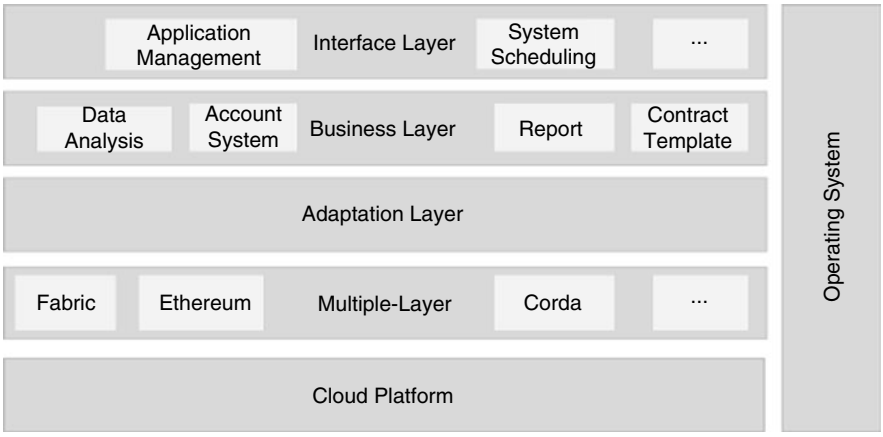


Fig. 4 Cloud platform connection with layering management

function calls will boost the cost of services unless users are cautious about their requests.

The advantages of serverless computing include:

- Scalability: Auto-scalability is provided in most serverless settings, rendering scalable solutions an absolute science.
- Agility: CSPs build systems that in short release cycles and produce solutions.
- Faster time to market: In-house teams do not have to wait for massive investments and costly IT processes to turn their innovations into marketable solutions.
- Disaster Response Time: Recovery is almost immediate after an outage, which decreases costs and effort.
- With FaaS
- FaaS: From server farms to serverless computing, the key distinction among server-based and serverless computing is that organizations can now pay for billable requirements in the context of functions rather than always executing in-house code. The most lucrative aspect of serverless computing is that it really brings all the issues out of managing and controlling the infrastructure and related infrastructure, leaving the emphasis on requesting FaaS services appropriately.

It can take a little getting used to, but in the end, business users can get ready-made solutions to their everyday business issues without having to think about complicated IT configurations. For those organizations that have already chosen cloud for BI or other unique needs, serverless adoption rates could be higher [20].

5 Application of Blockchain in Cloud Computing

Popular users have been attracted by recent advances in information management systems to better store their data. The modern era of cloud computing is used by cloud users as a utility model. Depending on their properties, the cloud users can connect, share, or communicate the data anywhere, anytime. This implicitly means that after being uploaded to the cloud server, cloud users do not even have direct control over services. The cloud provider provides services as such and as available on the basis of terms and conditions. When we dive deeper into the information age in terms of length, speed, and variety of data on the Internet, a huge increase can be observed. Data may come from different types of sources, including mobile devices, sensors, files, and social networks (Fig. 5). This type of data explosion raises serious research questions such as how to handle vast volumes of data effectively and optimally and consider the new ways of unlocking knowledge preservation. Millions of transactions consisting of critical, heterogeneous, and homogeneous data are being generated that do not compromise the quality of end-user service. Challenges remain in supporting information processing units in various financial markets to

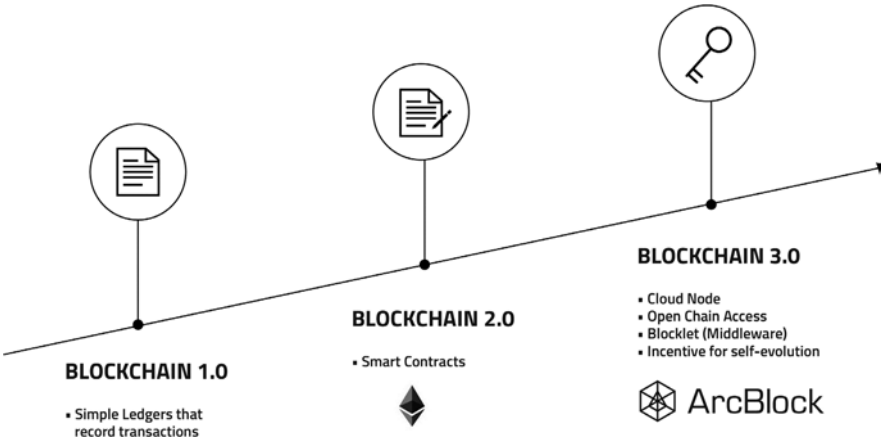


Fig. 5 Evaluation of blockchain milestone

build next-generation financial technologies for the safe use of network infrastructure and user communications. In order to deal with financial stability, blockchain technology has been implemented. It is defined as a network of public ledgers that offer better secured online transactions. The transaction process is mainly carried out via the authentication process through the blockchain principle, where the customer conducts virtual transactions. This block is constantly updated and mirrored in the details of the electronic money transaction to share the current block of transaction details [21].

5.1 Bitcoin Concept

(a) Initially, fresh transactions are broadcast to so many nodes.
(b) The new transaction is collected by each block point.
(c) Proof of work should be allocated to any block.
(d) If node-based proof of work is found, then broadcast messages are sent to all nodes in that block (Fig. 6).
(e) Only valid, rather than expended, transactions are processed.
(f) Nodes, centered on their cryptographic facilities, accept the blocks.

To apply the blockchain into cloud systems, there are two methods available:

(a) Blockchain integration with the cloud to enable enterprise networks such as storage
(b) Blockchain replication [22, 23]

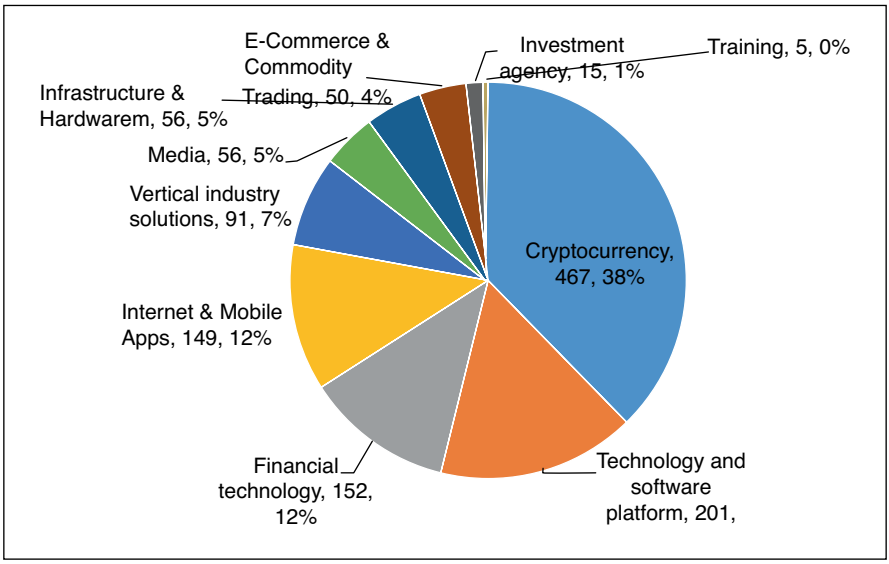


Fig. 6 Graphical representation of various domains on Bitcoin

5.2 Transactional Database Access and Permission

(a) Alignment between mission, user, and data management in clouds with security principles

The issues and specifications involved in facilitating cloud-based blockchain transactions are as follows:

(a) In view of security: data is shielded from the user and stored in data centers. Therefore, for tuning purposes, transactional operations should be allocated. This implies that the cloud service enables its users to have control over the places where their information is stored and processed.
(b) System reliability and fault tolerance: the system should be able to locate an alternative node if there is a network failure of either node, thus, in data centers, a node replication process and the use of several software applications.
(c) Protection for blockchain improvements: In distributed cloud environments, apps should be centrally delegated, and multiple software applications should be used [24, 25].

6 Blockchain-as-a-Service Expedites Land-Based Applications

The integration of blockchain and cloud computing would minimize blockchain implementation costs effectively. Pre-configured networks, traditional blockchain infrastructure, similar information security, distributed lower business-reliable monitoring logic, similar node connection logic, etc. seem to be, on the one hand, embedded and differentiated as blockchain services to serve various customers in the upper application layer. Fast development of cloud computing blockchain services will carry out rapid verification of concepts and model feasibility. Cloud computing paid by use on the other hand allows the use of basic infrastructure resources or adapts to meet the actual requirement to speed up the development phase of software, minimize implementation costs, and satisfy the service request in the potential blockchain community of start-ups, academic institutions, open-source groups, alliances, and financial institutions (Fig. 7).

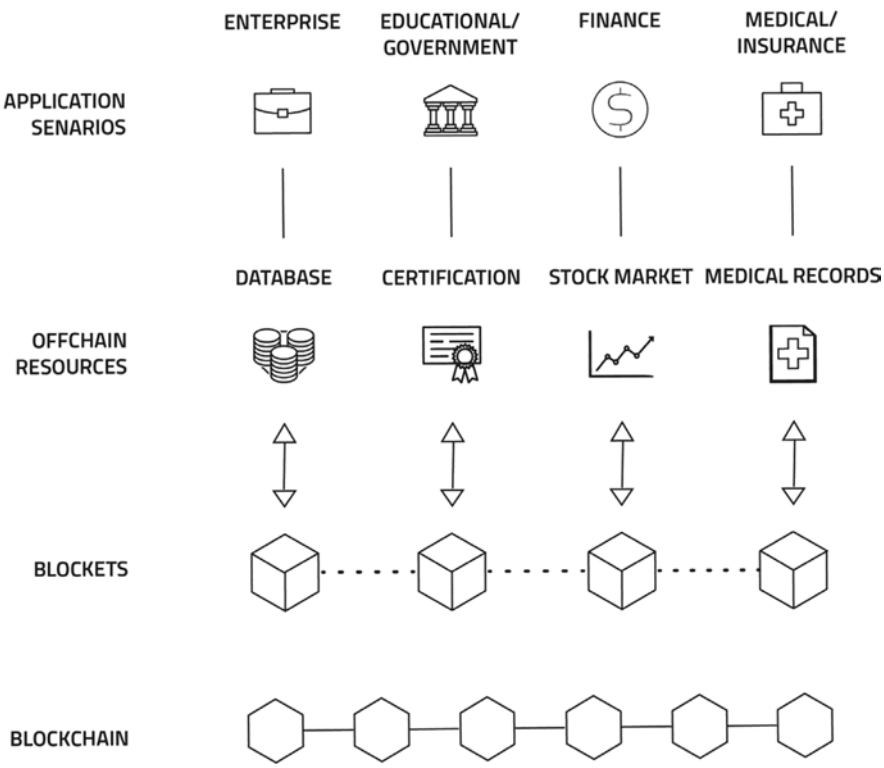


Fig. 7 Fields of blockchain collaboration with cloud computing

Blockchain collaborated with cloud technology to build blockchain-as-a-service (BaaS), based on the three types of services currently offered by cloud computing (IaaS, PaaS, SaaS). BaaS network operators aim to offer better blockchain services to customers, such that BaaS network operators pay more attention to linking vertical businesses than providers of blockchain infrastructure technology to provide fair reference implementation models, effective account system capital and performance management system, and personalized data analysis and performance reports [26].

6.1 Computing Serverless

Serverless computing is an application built for cloud computing in which the cloud provider handles the assignment of computing resources continuously. Most serverless vendors provide platforms that execute application programs but do not collect information for computational runtimes or act as a service (FaaS).

Including blockchains, serverless computing frameworks also work well. Most of the blocklets can be introduced as a serverless program. Use AWS Lambda, Windows Azure Functions, or another serverless execution environment to handle blocklets. Remember that various levels of abstraction include microservice architecture and serverless computing. A microservice that perfectly suits into a virtualized environment can be introduced by serverless computing. Development teams however can leverage serverless computing for many other purposes as well, and the use of serverless technology to incorporate microservices is not always necessary [27, 28].

Changing the blockchain topology to a transaction-based directed acyclic graph (DAG) is the first type of high-performance solution. Under this topology, the whole network is confirmed by the broadcast to form a transaction network after the transaction request is initiated. There is no packaging process, and it is possible to strip the transaction from the network or merge it back together. There is no block definition for DAG-based designs, and expansion is not constrained by block size (Table 1). The scalability depends on the bandwidth of the network, the speed of

Table 1 Classification of serverless computing

Classification	Notary	Sidechain/relays	Hash-locking
Inter-blockchain	Bidirectional	Bidirectional/Unidirectional	Bidirectional
Asset exchange	Support	Support	Support
Asset transfer	Support	Support	Support
Trust	Require the third party	No require	No require
Type	Protocol	Technology architecture	Algorithm
Difficulty	Average	Hard	Easy
Use case	Ripple	BTC relay Polkadot COSMOS	Lightning network

CPU processing, and the limitations of storage capacity. This topology tackles security concerns, issues of high competitiveness, problems of scalability, and problems of data growth and adapting to micropayment scenarios [29].

7 The Current Blockchain Situation

Blockchain is acknowledged by several nations who are pursuing the popularization and implementation of technology in many fields. On January 25, 2019, Innovate UK employees said that the United Kingdom will spend 19 million to help emerging products or services such as blockchain in nascent technology fields. On February 12, 2019, in the United States, the second blockchain hearing was held by the House of Representatives, and a consensus was reached on the concept of these technologies: it should not be promoted but smothered. The Bank of Korea supports blockchain technology, and the only South Korean stock exchange, Korea Exchange (KRX), has also announced the launch of a blockchain technology-based trading platform. Blockchain technology is currently being pursued in Australia in different fields. And blockchain technology has already been applied by Australian Post to identity recognition. The Global Blockchain Committee and a coalition of over 30 members have been established in Dubai, including Cisco, blockchain start-ups, and the government of Dubai [30–32].

8 Improve the Blockchain Development Policy Climate

The effect of the blockchain on the security of personal information and cross-border data flow will be extensively studied, and the regulatory concerns of the blockchain will be addressed in the underlying core technology, mid-level application logic, and top-level information management and control. And we will actively encourage the disclosure of information by the blockchain system participants, create a compliance evaluation and audit process for smart contracts, and promote self-discipline in the industry. At the same time, relevant blockchain policies and laws and regulations should be studied, and in order to create a good environment for the healthy development of the industry, the supervisory mechanisms and certification systems for the technology and application of the blockchain should be explored [33–36].

Bitcoin Provides Proof of Authenticity in a Weak Form: Since the blockchain of Bitcoin is an irreversible ledger, it can be considered that proof of authenticity should be simple. For example, a manufacturer could log the authenticity certificate's cryptographic fingerprint to the blockchain and provide a reference ID to the reseller/customer that allows the reseller/customer to see the authenticity certificate on the blockchain (Fig. 8). The issue is that Bitcoin is an open ledger and fingerprint content can be fed by anyone, even counterfeiters [37].

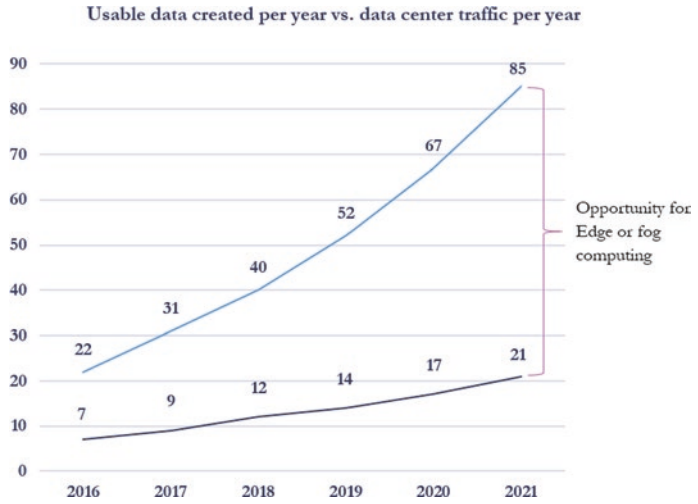


Fig. 8 Traffic record in yearwise

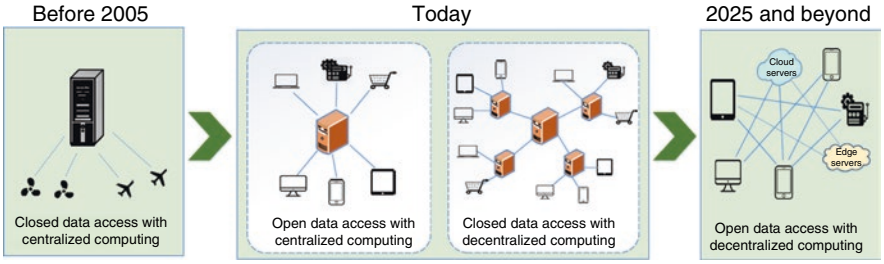


Fig. 9 Data access with centralized and decentralized computing

9 Decentralized Approaches and Challenges Faced Based on Blockchain

Some approaches include ensuring that the correct incentivization strategy is in effect for resource providers by establishing equal allocation of revenue and keeping the technology scalable, taking into account the existing scalability limitations of blockchain infrastructures. Machine testing is done correctly to avoid future malicious attacks (i.e., a provider claiming to have provided the service without effectively doing it). Some ventures use methods of reputational management, but these methods need to provide the right balance between the weight of reputations and the cost of market entry (Fig. 9).

Use trusted oracles*, since true sight by natural environment is not decentralized. In the event of premeditated users or other (common) inconvenience, there are centralized suggestions for immortals that could alleviate the confidence problem of managing the right to erase data [38, 39].

9.1 Decentralized Cloud Solutions Focused on Blockchain

Cloud computing has traditionally been developed by creating virtual machines, emulations that make it more difficult to operate on hardware, which is definitely one computer but appears to be several separate computers [40–42]. It takes a lot of device resources (CPU and RAM) for virtual machines to run, minutes from start, and complicated resource management for software creation. Containerization, on the other hand, only virtualizes a computer's operating system, in order to allow distributed applications to run on each implementation without launching an entire virtual machine (VM). It takes only seconds for containers to start as well as the underpinning orchestration mechanism, which further continues the interrelationships and interactions between cloud infrastructure workloads and allows for easier and faster management of resources for software development. Furthermore, TEE, including Intel SGX, allows an implementation to be executed inside graphics card communities or memory-protected execution areas that increase security even on compromised platforms. This infrastructure can testify to the useful calculation of the miners for the system and as such provide rewards accordingly [43, 44].

9.2 Decentralization

With its distributed nature, blockchain is a promising methodology to solve bottleneck and single-point failure problems effectively by removing the need for a trusted third party in the CoT network. Furthermore, the blockchain peer-to-peer architecture enables all network members to check the correctness of IoT data and ensure immutability with fair validation rights. Security and privacy: By using blockchain-enabled smart contracts, the BCoT system can achieve trustworthy access control that enables all operations of cloud providers and IoT devices to be automatically allowed and avoids possible threats to cloud resources and improves fine-grained control of IoT data. In addition, the blockchain allows users to monitor their network transactions in order to preserve device and data ownership to improve the privacy of information [45].

On the cloud platform, decentralized blockchain-based cloud storage can be created via its hash values (Fig. 10). Blockchain-based storage manages IoT data and regularly implements verification to identify the potential for data alteration, for example, the InterPlanetary File System (IPFS) [46].

It is a blockchain-based database system that can be safely stored between storage nodes and is now available on the cloud. This has also been shown to address effectively data storage problems brought by centralized cloud models in terms of data leakage and storage management.

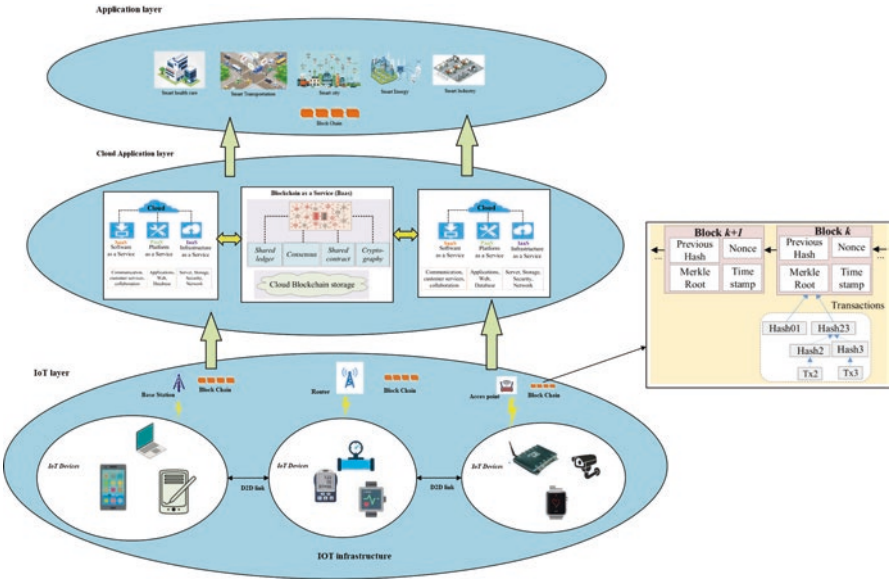


Fig. 10 Interlinking of various layers with blockchain

9.3 Applications from BCoT

CoT allows efficient exchange of health data in environments where EHRs can be collected and stored electronically on cloud servers, while consumers can access their medical records for health tracking using their mobile devices (e.g., smartphones). This promises to deliver healthcare services on demand, save healthcare costs, and enhance the quality of experience. However, due to attack potential and lack of trust between health cloud providers, cloud storage, and users, health data sharing based on such complex cloud IoT environments is often susceptible to security and privacy risks. Via decentralized data verification of all peers and message confirmation based on consensus frameworks, blockchain plays an important role in solving safety issues in health data sharing. In particular, blockchain traceability enables healthcare institutions (e.g., healthcare providers, insurance firms, and patients) (Fig. 11) to monitor user access habits and identify data attacks in order to strengthen the protection of exchange of health data in BCoT networks [47, 48].

Overlay networks, cloud storage servers, healthcare providers, smart contracts, and patients make up the architecture. In particular, the blockchain is linked through a P2P network to cloud storage, where each cloud storage holds medical records in blocks and the hash value of these.

Blocks are stored in a series of blocks. This makes it possible to easily track any changes in details.

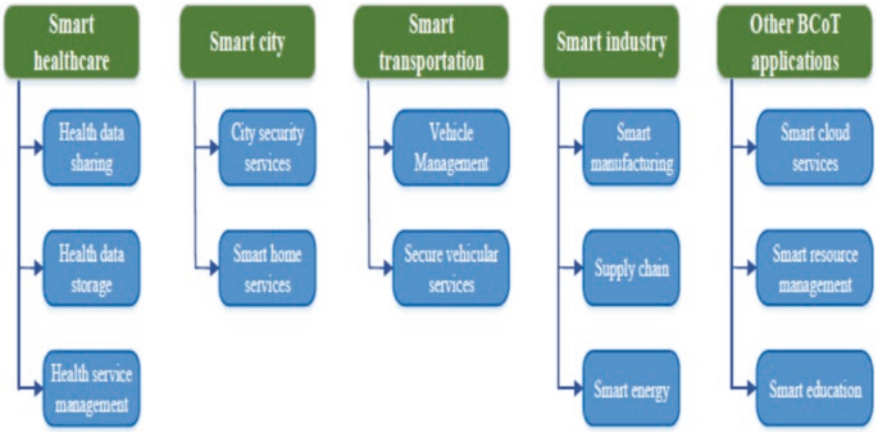


Fig. 11 Hierarchal structure of blockchain fields in the current environment

10 Conclusion

We defined the design and the architecture priorities of three decentralized cloud systems in this chapter. In addition, we measured them, addressed future work gaps in the field, and underlined the need for a number of features to be standardized. Blockchain-based cloud initiatives are still in their development, and so many open limitations need to be tackled, such as computational performance validation and company resource benchmarking. The schemes under consideration concentrate on the production of a functional product with a view to commercial solutions, and usability is one of their key indicators of performance. In the long run, however, the lack of standards could become an obstacle to competing with big suppliers and could impede the development of open markets.

References

1. C. Xu, K. Wang, M. Guo, Intelligent resource management in blockchain-based cloud datacenters. IEEE Cloud Comput. **4**(6), 50–59 (2017)
2. Y. Zhang, R.H. Deng, X. Liu, D. Zheng, Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. Inf. Sci. **462**, 262–277 (2018)
3. C. Yang, X. Chen, Y. Xiang, Blockchain-based publicly verifiable data deletion scheme for cloud storage. J. Netw. Comput. Appl. **103**, 185–193 (2018)
4. R. Zheng, J. Jiang, X. Hao, W. Ren, F. Xiong, Y. Ren, bcbim:A blockchain-based big data model for bim modification audit and provenance in mobile cloud. Math. Probl. Eng. **2019** (2019)
5. J. Ricci, I. Baggili, F. Breitinger, Blockchain-based distributed cloud storage digital forensics: Where's the beef? IEEE Secur. Privacy **17**(1), 34–42 (2019)
6. Y. Ren, Y. Liu, X. Yin, Z. Shen, H.-J. Kim, Blockchain-based trusted electronic records preservation in cloud storage. Comput. Mater. Continua **58**(1), 135–151 (2019)

7. Z. Li, Z. Yang, S. Xie, Computing resource trading for edgecloud- assisted internet of things. IEEE Trans. Ind. Inf. **15**(6), 3661–3669 (2019)
8. Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, Z. Han, Cloud/fog computing resource management and pricing for blockchain networks. IEEE Internet Things J. **6**(3), 4585–4600 (2018)
9. S. Nayak, N.C. Narendra, A. Shukla, J. Kempf, Saranyu: using smart contracts and blockchain for cloud tenant management, in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, (IEEE, 2018), pp. 857–861
10. A. Alammary, S. Alhazmi, M. Almasri, S. Gillani, Blockchainbased applications in education: a systematic review. Appl. Sci. **9**(12), 2400 (2019)
11. M. Hori, M. Ohashi, Adaptive identity authentication of blockchain system-the collaborative cloud educational system, in *EdMedia+ Innovate Learning. Association for the Advancement of Computing in Education (AACE)*, (2018), pp. 1339–1346
12. SONM supercomputer organized by network mining, White Paper, SONM (2017) [Online]. Available: https://github.com/masonicGIT/ico-whitepapers/blob/master/sonm/sonm.pdf
13. C. Cerin, G. Fedak, *Desktop grid computing* (CRC Press, Boca Raton, 2012)
14. J.R. Douceur, The sybil attack, in *International Workshop on Peerto- Peer Systems*, (Springer, Cham, 2002), pp. 251–260
15. R. Canetti, B. Riva, G.N. Rothblum, Practical delegation of computation using multiple servers, in *Proc. of the 18th ACM Conference on Computer and Communications Security*, (ACM, 2011), pp. 445–454
16. S.T. Setty, R. McPherson, A.J. Blumberg, M. Walfish, Making argument systems for outsourced computation practical (sometimes), in *Proc. of the NDSS*, vol. 1, (Springer, Cham, 2012), p. 17
17. V. Scoca, R.B. Uriarte, R. De Nicola, Smart contract negotiation in cloud computing, in *Proc. of the 10th IEEE Cloud Computing*, (IEEE, 2017), pp. 592–599
18. R.B. Uriarte, F. Tiezzi, R.D. Nicola, SLAC: a formal service- level-agreement language for cloud computing, in *Proc. of the 7th IEEE/ACM UCC*, (2014), pp. 419–426
19. R.B. Uriarte, S. Tsaftaris, F. Tiezzi, Supporting autonomic management of clouds: Service clustering with random forest. IEEE Trans. Netw. Serv. Manage. **13**(3), 595–607 (2016)
20. A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification (ws-agreement), in *Open grid forum*, vol. 128, (Springer, Cham, 2007), p. 216
21. R.B. Uriarte, F. Tiezzi, R. De Nicola, *Dynamic SLAs for Clouds* (Springer, Cham, 2016), pp. 34–49. https://doi.org/10.1007/978-3-319-44482-63
22. B. Yin, L. Mei, Z. Jiang, K. Wang, Joint cloud collaboration mechanism between vehicle clouds based on blockchain, in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, (IEEE, 2019), pp. 227–227
23. Y.J. Ren, Y. Leng, Y.P. Cheng, J. Wang, Secure data storage based on blockchain and coding in edge computing. Math. Biosci. Eng. **16**, 1874–1892 (2019)
24. Barenji, A. V., Guo, H., Tian, Z., Li, Z., Wang, W. M., & Huang, G. Q.. Blockchain-based cloud manufacturing: decentralization. arXiv preprint arXiv:1901.10403 (2019)
25. J. Lee, M. Azamfar, J. Singh, A blockchain enabled cyber-physical system architecture for industry 4.0 manufacturing systems. Manuf. Lett. **20**, 34–39 (2019)
26. K. Gai, Y. Wu, L. Zhu, L. Xu, Y. Zhang, Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks. IEEE Internet Things J. **6**(5), 7992–8004 (2019)
27. S. Cao, G. Zhang, P. Liu, X. Zhang, F. Neri, Cloud-assisted secure eHealth systems for tamperproofing EHR via blockchain. Inf. Sci. **485**, 427–440 (2019)
28. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, Boca Raton, 2020), pp. 1–23
29. Z. Li, X. Liu, W.M. Wang, A. Vatankhah Barenji, G.Q. Huang, CKshare: Secured cloud-based knowledge-sharing blockchain for injection mold redesign. Enterp. Inf. Syst. **13**(1), 1–33 (2019)

30. A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, D. Zheng, Efficient and privacy-preserving traceable attribute-based encryption in blockchain. Ann. Telecommun. **74**(7), 401–411 (2019)
31. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global, 2021), pp. 165–177
32. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, Boca Raton, 2020)
33. Farhadi, M., Miorandi, D., & Pierre, G.. Blockchain enabled fog structure to provide data security in IoT applications. arXiv preprint arXiv:1901.04830 (2019)
34. R. Chandran, S.R. Kumar, N. Gayathri, Genetic algorithm-based tabu search for optimal energy-aware allocation of data center resources. Soft. Comput. **24**(21), 16705–16718 (2020). https://doi.org/10.1007/s00500-020-05240-9
35. R. Chandran, S.R. Kumar, N. Gayathri, Designing a locating scams for mobile transaction with the aid of operational activity analysis in cloud. Wirel. Pers. Commun. **29**, 123–141 (2020)
36. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2, in *Blockchain, Big Data and Machine Learning: Trends and Applications*, (CRC Press, Boca Raton, 2020), p. 97
37. K. Gai, Y. Wu, L. Zhu, M. Qiu, M. Shen, Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans. Ind. Inf. **15**(6), 3548–3558 (2019)
38. L. Il-Kwon, K. Young-Hyuk, L. Jae-Gwang, L. Jae-Pil, The analysis and countermeasures on security breach of bitcoin, in *Proceedings of the International Conference on Computational Science and Its Applications, Guimarães, Portugal, 30 June–3 July 2014*, (Springer International Publishing, Cham, 2014)
39. A. Beikverdi, S. JooSeok, Trend of centralization in Bitcoin's distributed network, in *Proceedings of the 2015 16th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), Takamatsu, Japan, 1–3 June 2015*, (2015)
40. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
41. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195
42. R.K. Sakthivel, G. Nagasubramanian, F. Al-Turjman, M. Sankayya, Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry, in *Transactions on Emerging Telecommunications Technologies*, (2020), p. e3947
43. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten, Sok: Research perspectives and challenges for bitcoin and cryptocurrencies, in *Proceedings of the 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 17–21 May 2015*, (2015)
44. K. Christidis, D. Michael, Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016)
45. H. Huang, X. Chen, Q. Wu, X. Huang, J. Shen, Bitcoin-based fair payments for outsourcing computation of fog devices. Future Gener. Comput. Syst. **78**, 850–858 (2016)
46. S. Huh, C. Sangrae, K. Soohyung, Managing IoT devices using blockchain platform, in *Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017*, (2017)
47. F. Armknecht, G. Karame, A. Mandal, F. Youssef, E. Zenner, Ripple: overview and outlook, in *Trust and Trustworthy Computing*, ed. by M. Conti, M. Schunter, I. Askoxylakis, (Springer International Publishing, Cham, 2015), pp. 163–180
48. M. Vasek, T. Moore, There's no free lunch, even using bitcoin: tracking the popularity and profits of virtual currency scams, in *Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015*, (Springer, Berlin/Heidelberg, 2015)

Blockchain Technology: A Boon at the Pandemic Times – A Solution for Global Economy Upliftment with AI and IoT

P. R. Anisha, C. Kishor Kumar Reddy, and Nhu Gia Nguyen

Abstract Blockchain technology is a potential sector at the foreground, though it is currently in its embryonic form, but will retain itself as an emerging technology at an early stage. Besides blockchain being a trusted, decentralized database, it has its success in many applications across various fields like education, medicine, insurance, finance, energy, environment, supply chain management, and various other associated operations. The work provides a systematic survey of blockchain, how it works, and its characteristics, applications, and challenges. The aim is to investigate how blockchain technology, besides artificial intelligence and the Internet of Things, would be an effective factor to fight the current pandemic scenario. To the end, a brief survey is carried out on how blockchain technology would be fruitful in uplifting the global economy post-COVID, with a summary of the blockchain toolkit by the World Economic Forum.

Keywords Artificial intelligence · Blockchain technology · Economy upliftment · Internet of Things · Pandemic support · World Economic Forum

1 Introduction

For the first 40 years of its evolution, the Internet has fetched us many progressive things. As the time progresses, the Internet has evolved so much that it has permitted using e-mail, the World Wide Web (WWW), numerous social media platforms, big data, Internet of Things, cloud computing, and mobile applications. With the advent

P. R. Anisha · C. K. K. Reddy (✉)
Duy Tan University, Da Nang, Vietnam

N. G. Nguyen
Graduate School, Duy Tan University, Da Nang, Vietnam

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_11

of the Internet, its existence has brought a lot of positive outcomes to every field of work at large. Right from the use of the World Wide Web to the emails, mobile applications, social media, and the Internet of Things, the internet has brought many changes with its dynamism. Besides its pros, the Internet also carried many varied hindrances like privacy, security issues, intrusions, inclusion, management of data, accounts, ledgers, and even currency transactions. For example, in the field of online transactions, there is payment through bank or credit card, and in either cases, a third party or a middleman is involved in the transaction. This indirectly indicates that there are two entities involved: one id the bank, as all data is centralized, and the other is a third-party organization that maintains the same. In order to avoid the same, blockchain helps to solve such issues. In short, blockchain maintains the growing list of records of data which are authenticated by the nodes making use of it. It is a decentralized solution which removes the dependency on a third-party organization. The data is maintained in the form of public ledgers, and every transaction is stored in the form of chunks or blocks. As the data increases, the blocks keep increasing, thus moving as a chain. In order to conserve the security and stability over the ledgers, distributed consent algorithms and distorted cryptography are used. The crucial characteristics of using this technology are decentralization, auditability, persistency, and anonymity. The increase in decentralization makes the system more secure. Maintaining these characteristics allows the blockchain to save money while remaining efficient.

Besides its advantage in transaction, the use of blockchain is found to be fruitful in various fields such as crowdfunding [1–3], goods tracking in supply chain [4–6], authentication [7], voting services [8], cryptocurrency, etc. The use of blockchain technology has expanded beyond digital currency and finance to include smart energy, supply chain management, market monitoring, healthcare, and copyright protection. It has also gained a lot of attention in the fields of charities and nonprofits, arts, financial sector, e-commerce, etc. Business makes use of blockchain to attract customer and preserve their reliability and honesty. Besides Bitcoin and other cryptocurrencies being the best example for blockchain technology, the distributed ledger technology has also paved its way as a technological example for blockchain. Depending on who has access to the blockchain network, authorizations are further assigned and this is done in four categories:

The public/unrestricted blockchain network
The private/restricted blockchain network
The permissible blockchain network
The conglomerate blockchain network

The Public/Unrestricted Blockchain Network This network is open to any individual who wants to join and use it, e.g., Bitcoin.

The Private/Restricted Blockchain Network It is similar to the public blockchain in that it is also a decentralized peer-to-peer network, with the exception that

Table 1 Comparison of public, private, and consortium network

Specificity	Public	Private	Consortium
Read permission	It is public	Private, could also be made public with restrictions	Could be made public or private with restriction
Efficiency	Less efficient	Highly efficient	Highly efficient
Centralization	Not centralized	Can be centralized	Partially centralized

it is governed by one firm. The firm which governs the network executes the consensus protocol and maintains the logs in the form of mutual records.

The Permissible Blockchain Network This can be used in the private or public blockchain network, where the firm decides its constraints on who is permitted to participate in the network or what transactions can be leveraged to the participants.

The Conglomerate Blockchain Network It is ideal for businesses where all participants need to be permissioned to share the responsibility of the blockchain, meaning that individuals who may access or make transactions over the given data must be granted access (Table 1).

1.1 Work of a Blockchain

Blockchain is a sequential array of blocks that can hold a wide range of transactional records like a conventional unrestricted ledger [9]. The architectural representation is given in Fig. 1.

A block comprises of the block header and the block body as shown in Fig. 2.

(i) Block version: It represents the block validation rules to be followed.
(ii) Merkle tree root hash: It gives the hash value in the block for all the transactions.
(iii) Timestamp: It represents the current time.
(iv) nBits: It gives the threshold of a block hash.
(v) Nonce: It is a 4-byte field that starts from 0 and increments with each hash calculation.
(vi) Parent block hash: It is a pointer to the previous block holding a 256-bit hash value.

The structure of the block further comprises of transactions and transaction counter. The amount of transactions a block has is dependent on the size of the block and the size of the transaction. Blockchain uses a distorted cryptography methodology to authorize the authentication of transactions [10]. Digital signature based on distorted cryptography is used in unreliable environments.

An architectural representation of how blockchain works is shown in Fig. 3.

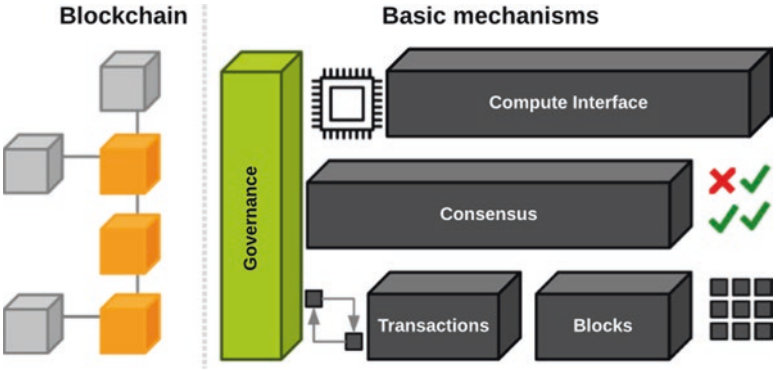


Fig. 1 Blockchain architecture [9]

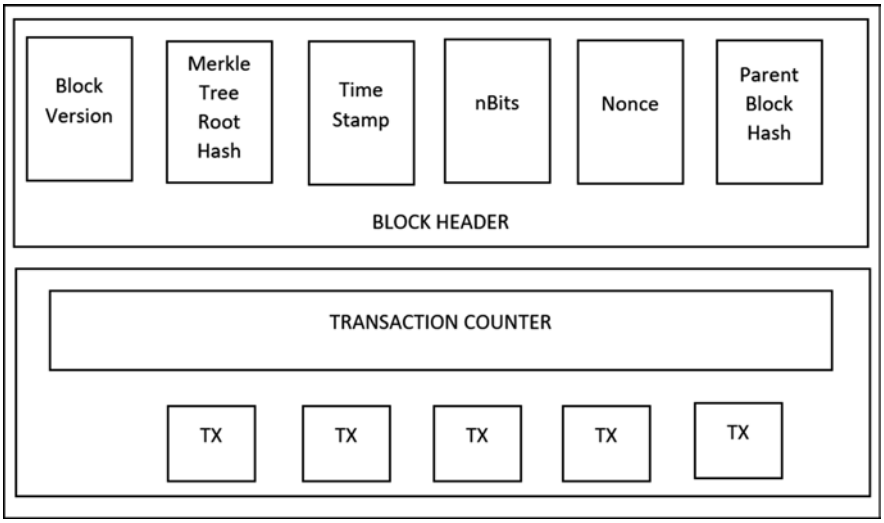


Fig. 2 Structure of blockchain

1.2 The Significant Characteristics of Blockchain

Decentralization In conservative consolidated transaction systems, each transaction must be authenticated by a central trustworthy organization (e.g., the central bank), unavoidably resulting in rate and performance bottlenecks at the central servers. In comparison to the centralized mode, the use of third party is currently no longer needed in blockchain. Consent algorithms in blockchain are used to conserve data reliability in circulated network.

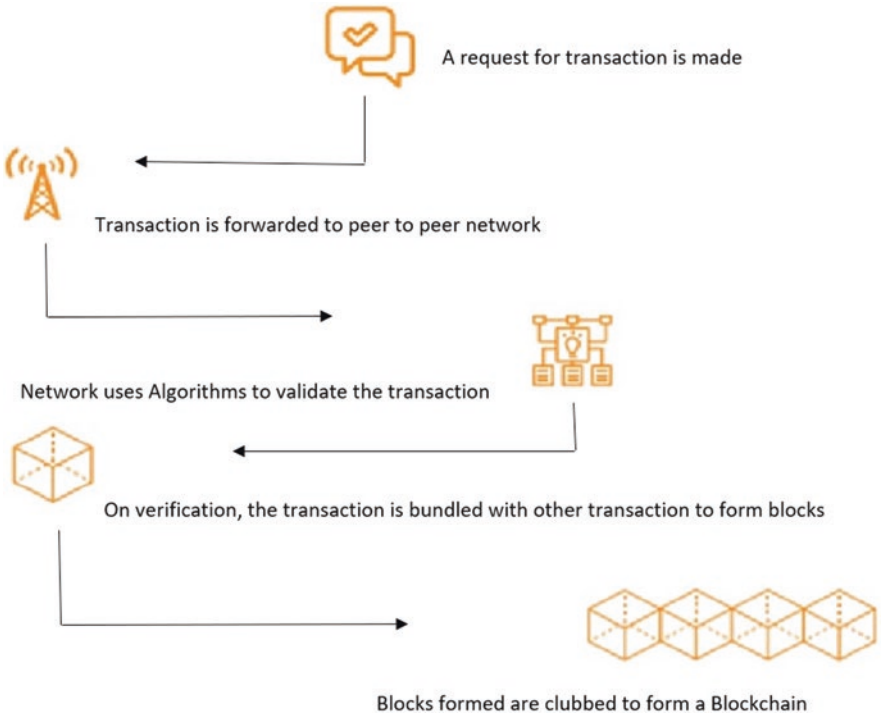


Fig. 3 An architectural representation of how blockchain works

Persistency Transactions can be authorized rapidly, and unacceptable transactions would not be acknowledged by genuine miners. It is approximately impossible to erase or rollback transactions once they are included in the blockchain. Blocks that contain unacceptable transactions could be revealed immediately.

Anonymity Any customer can communicate with the blockchain using a provided address, which does not disclose the existent identity of the customer. Remember that blockchain cannot assure the faultless confidential safeguarding due to the inherent restraint.

Auditability Bitcoin blockchain stocks records of customer positions grounded on the unaccessed transaction output (UTXO) methodology [2]: any transaction has to give reference to a few forgoing unspent or unaccessed transactions. Once the latest transaction is logged into the blockchain, the state of those referred unaccessed transactions alternates from unspent to spent or unaccessed to accessed. So, transactions could be easily authorized and traced.

2 Literature Survey

The earlier traditional business process that worked on a centralized architecture or relied on a third party for their applications or transactions is not disrupted due to blockchain as the same task could be handled in a decentralized manner by maintaining the same pace of certainty. This paradigm shift of blockchain has eventually migrated business from end-to-end principle to trust-to-trust principle [11]. In order to maintain the trust, such a network provided by blockchain can be given assistance in a crystal clear mode, which holds itself accountable for handling errors or malfunctioning of some other category. Apart from having a network, blockchain further benefits the organization to interact among various stakeholders for its operations as it avoids third party and creates transparency through its non-trusting environment. This benefit of blockchain has made various industries, such as the energy sector, finance, insurance, logistics, and transport, turn their business toward blockchain technology for automatization [12–16]. On the other hand, apart from the immutable premise, transparency, and peer-to-peer consensus that blockchain provides, it also puts forth a platform providing a trusted audit for the network systems handing the control even to the edges of the network [17].

Blockchain technology has further given rise to crypto-economy, which further is implemented by a non-tokenized scheme. The use of blockchain taxonomy and hybrid solutions are given priority to move from permissionless to permissioned blockchain network to the public permissionless ledgers where trust is a paramount [18]. For a long time, cryptocurrency has been a successful blockchain-based example termed as Bitcoin. It stood as a protocol which enabled transactions to take place on the Bitcoin blockchain network systems. It worked on the basis of Bitcoin digital currency symbolized as BTC [19]. Besides the detailed taxonomy of blockchain technology which helps in choosing the right architecture of blockchain for an organization, it further helps in configuring based on various parameters such as cost efficiency, flexibility, performance, blockchain storage, computation, and the degree of decentralization [20]. Research provides various comprehensive overviews of the upcoming blockchain architectures, how it stands distinct from the existing traditional databases, and electronic exchange mechanism [16]. Based on the organizational investment capability, privacy requirements, and real-life situations, the organization can make wiser choice where it would allow its business to work upon: the non-public block, the fully private blockchain, or the consortium blockchain network [21].

Among all the blockchain technology, Bitcoin has always coined its way as it is a mechanism to conduct a hassle-free business globally without an access to physical banking system with fiat foreign currency availability [18]. Research work has also concentrated on allowing to have transactions that can even carry storing instructions, sharing data, and queuing them. Its main utility is shown in mobile applications where user data like messages, pictures, and contacts needs lots of transactional and privacy support [22]. In the field of education as well, blockchain stands as a transformational force. Blockchain can provide easy sharable, verifiable,

and permanent record of educational data and rewards. This can be handled by having the educational reputation currency which institutions can opt for so as to be awarded to promote learner reputation [23]. Blockchain can be further used as a distributed system; its utility as an autonomous pension fund, which helps in running self-contract constructed system so as to cope with pension treasuries without having a principal trustworthy pension fund, has proven to be fruitful. As there are many activities related to this fund, like accepting payments from currently active clients, taxes and payments to legatees are part of this pension fund. In such a case, rather than lying on the currency issues in a global front, the same task can be accomplished by using self-execution bonds and cryptocurrency methodology. For this, Ethereum algorithm is put forth which requires event insurance related to life events from other trusted bodies as their prerequisite [24]. In the sector of healthcare, researchers have proposed the use of restricted/private blockchain to secure the medical information which is in the form of numeric, textual, image, or video which is handled by patients or any physician [25].

Research has proposed a blockchain-dependent system called MeDShare, which not just helps in sharing the medical information midst the cloud benefactors but is also responsible for information administration and authorization, derivation, and assisting support. This stands as a smart contract for detecting information behavior from information access patterns and even terminates spiteful users from accessing the confidential information, thus providing privacy [26]. Having various application-oriented advances of using blockchain technology, studies have also been focused on improving the scalability of blockchain by optimization of parameters like block size, construction of blocks, transaction security, and time control which leads to provide better performance in a cost-effective manner [27]. Having worked on scalability, efforts are even made on experimenting on the budget of stowage and business calculation practices for a standardized cloud environment with that of a blockchain environment. Results have shown that the costs on a single business process were higher on blockchain using Ethereum than that of Amazon. However, as the experiment was carried out on a restricted scope of sole business practice, the outcomes were not much indiscriminate, keeping in view the progresses that blockchain technology is making on a day-to-day progress, focusing on its optimization mechanism [28].

3 Blockchain: Trust Techniques, Applications, and Challenges

3.1 The Trust Techniques

The basis on which blockchain holds itself trustworthy depends on three elements: (1) identity, (2), ownership, and (3) verification.

1. *Identity*: In order to maintain the authenticity of any transaction, blockchain makes use of digital signatures so as to uphold the identity. This is carried by making use of the basics of cryptography, i.e., the use of private key and public key.
2. *Ownership*: In order to handle the ownership strategy, blockchain makes use of a technology named cryptographic hashing. As the structure of blockchain shows it holds a concept of hashing, here a math function is maintained; any change in the math function helps to identify the fraudulent between the blocks. This helps blockchain to generate immutable data also called as tamper-proof records.
3. *Verification*: A technique called "distributed consensus" is used to solve the verification problem which helps a set of people to publicly figure out if their transactions were apt. This would also lower the cost for many applications.

3.2 Application in Real World

Blockchain in Agriculture About 60% of the agricultural sector is shifting toward blockchain in order to curb the food fraud and increase the efficiency and transparency. It helps in the ignorance of a third-party approach in tracking, collecting, and managing the data of an agricultural supply chain. This helps in maintaining a proper traceability, managing data, and collecting of goods supply chain from farmers to customers.

Blockchain in Democracy and Governance In the voting system, blockchain helps to maintain the legitimacy and verify citizen identity. Voting can be carried out via the tokens on the blockchain, tracing the votes and simultaneously carrying out the counting. In terms of government data exchange, the distributed ledger technology could be an added advantage. The data of a citizen can be stored, making it harder to have incorrect data or make constant changes over it, thanks to the blockchain network, which helps constantly in not approaching the individual for their data and maintaining privacy and security over the exchange of data. In this regard, the government is forwarding itself toward this technology given the technological added security.

Blockchain in Digital Identity Digital identity is one promising field where utmost concentration is to be given, as the use of user-centric database may lead to a rise in fraud, data fidelity, and lack of control over data access. At this juncture, blockchain plays a vital role as it has a key advantage over delivering a digital identity with increased efficiency, transparency, fraud detection, and low cost. As the data in blockchain is immutable, it makes it impossible for any kind of fraud over the data, though blockchain allows multiple users to store and interact with the same database, but all these are handled in the most secure way.

Blockchain in Energy, Environment, and Climate These sectors hold millions of transactions in terms of trade and energy distributional aspect, making blockchain a potential technology to use in these fields. With more data control and micro-optimization of energy, blockchain helps in improving the efficiency through its decentralized platform. As blockchain facilitates peer-to-peer transmission, for the energy resources, micro-grid development is important because it helps to deregulate the market, allowing peer-to-peer transactions of payments and energy.

Blockchain in Financial Inclusion As the trade and market of organizations grow globally, the traditional banking and financial systems create an obstacle for cross-border payments. In this term, blockchain acts as a best solution by abolishing the necessity of a few intermediate third-party supports for cross-border payments. In comparison to the traditional approach, blockchain stands as a resulting factor for real-time processing, reducing the settlement and foreign exchange risk.

Blockchain in Health Blockchain shows its advantage in healthcare by preserving digital health records and exchanging pharmaceutical supply chain. The advantage of blockchain of providing a decentralized and patient-centric heath record system is an added advantage that helps health assistants to keep track of patient treatment rather than having duplicated data from various resources. On the patients end, it also helps them to have a perfect treatment process based on the individual genetics, environment, and lifestyle. This further helps to have health data archives which can also be used for medical research by securing the personal information of the patients.

Blockchain in Land Rights Blockchain characteristics in providing efficiency, maintaining transparency, and handling fraud have majorly helped countries in their efforts to settle titled land areas by certifying information through blockchain technology. This encourages accountability in land registrations, and the data can be publicly made beneficial to avoid fraud. There could also be a record maintained to keep track of the trending prices, ownership, area measurements, sellers, and buyer information and to also support government planners.

Blockchain in Aid and Charitable Organizations As most of the non-government organizations or the non-profit organizations or foundation initiatives depend on monetary funds, 82% of such organizations are moving toward blockchain so as to enhance their transparency, reduce tax cost, and track and monitor fund transfers. This helps such organizations to keep track of the donor and the recipients and maintain the record of each of the activity.

Blockchain in Education In the field of education, may it be academic, institutional, or online, blockchain technology plays a pivotal role. The technology helps in maintaining and providing a more secured, immutable record of pupils – attendance, performance, certificates, transcripts, and so on. These records would have various organizations in the recruitment process and would help the pupils or the institution in reducing the administrative burden.

3.3 Blockchain Challenges

Regulating Currency In terms of using cryptocurrency, regulating the currency value on a global front stands as the biggest challenge. The day-to-day evolution of currency makes it difficult to transform from the ratified currency to e-money to digitalized and finally to cryptocurrency.

Scalability As a result of the dimension of blocks, either in unrestricted or unauthorized blockchain, it stands tedious to scale up the blockchain technology [29].

Handling the Capacity of Blockchain Having dense network, the number of tracks required becomes immense, and each track must be well-maintained in the blockchain, which at times gets difficult.

Locking of Funds As every track has funds locked within them, moving from one track to another also needs transferring funds to the new track, which causes hindrance to perform blockchain transaction and at times turns risky and expensive when handling different partners [30].

Anonymity It is found out that seven out of ten individuals contemplate Bitcoin to have a judicious unrecognizability ranging from moderate to extraordinary, even though its associated risks are from moderate to near the ground/low [31].

4 Blockchain with AI and IoT

4.1 Blockchain with AI (Artificial Intelligence)

The confluence of blockchain and artificial intelligence can bolster machine learning and empower artificial intelligence to create and exchange financial items. AI with its demand higher than ever before is sure to run on top of blockchain, expanding AI capacity and, in any event, making financial products. The concoction of the same is certain given the fact that they deal with date and delivering value. In addition, the secure fabric allows one to generate profound insights, creating priceless information and value.

The technology giant Microsoft is attempting to decentralize and make it work in tandem with blockchain. With this, the future will be open for ultra-affordable machine learning models to run seamlessly on handheld devices, like modern-day smartphones and laptops, and also create invaluable data and upgrade the present-day models. Significantly, individuals can utilize the AI models literally for free. Some of the numerous applications incorporate creating virtual assistants or recommending frameworks (e.g., what Netflix uses to suggest appears). Evidence of ideas was made using Ethereum.

Models can be refreshed on the blockchain or utilized off-chain on the client's neighborhood gadget at no exchange cost. The unchanging idea of blockchain and clean agreements implies that the model will consistently perform to specification. Organizations can set themselves up to create joined AI and blockchain arrangements by improving their computerized and information abilities. Computerized change or digital work is a forerunner to AI and blockchain selection. Overseeing information and business forms utilizing computerized frameworks furnishes AI activities with firm-wide information, empowering AI usage at scale.

Not exclusively can square affixes be utilized to share models and information, yet blockchains can help serve a job as an "ace mind" in a way shared over numerous AI frameworks. In the event that we can put these mutual learning benefits and blockchain and AI together, the chance may likewise be there to join these things that can gain from their environmental factors and afterward share that learning with all of the AI frameworks on the system. A significant advantage would be that nobody claims it and there's no administration power over the bot or the mutual cerebrum. It might be fair and impartial as a result of the sheer measure of data rolling in from various zones and various edges, a multidimensional holistic perspective. Another application is tending to the test of explainable AI. One of the more noteworthy issues with profound learning is that there is anything but a reasonable thought regarding what sources of information bring about what yield and how that influenced the entire arrangement. On the off chance that something turns out badly in a profound learning neural system, we don't have a way to recognize the issue and resolve it. This is the issue of neural systems in actuality being a "black box" with no genuine straightforwardness or logic. Notwithstanding, on the off chance that we use blockchains, we can record how individual activities bring about an ultimate choice in a non-trustworthy way, which permits us to return and see where things turned out badly and afterward fix the issue. The blockchain would be utilized to record occasions, for example, self-ruling vehicle choices and activities that won't be adjusted later. This can likewise build trust since the blockchain component is impartial and is only for capacity and examination, so anybody can go in and see what has occurred.

At last, AI frameworks can be utilized to improve blockchains when all is said and done. AI frameworks can watch out for what's going on in the blockchain. It can search for similar patterns in the kinds of information being put away and activities being performed on a specific server and being utilize to alarm clients when something might be occurring. The frameworks can search for typical conduct and banner what is by all accounts surprising. The AI frameworks can help keep blockchain progressively secure, increasingly solid, and progressively productive. While it's very conceivable that the universes of AI and blockchain are brimming with publicity, there are real, substantial, sensible manners by which

the two developing advancements can be utilized in ways that advantage one another and give genuine results to those hoping to actualize the innovations today in their surroundings.

4.2 Confluence of AI and Blockchain

The conjunction of AI in blockchain makes maybe what is the world's extremely dependable innovation empowered by a dynamic framework that is basically carefully designed and gives strong bits of knowledge and choices. It holds huge advantages which are as follows:

- Enriched business information methodologies
- Globalized authentication systems
- Groundbreaking inventories and compliance systems
- Smarter finance
- Apparent authority
- Intellectual merchandizing
- Intellectual predictive analysis
- Digital intellectual property rights

4.3 Blockchain with IoT (Internet of Things)

Blockchain has been substantiated for every objective and resolution and all examination practices as a rapidly growing expansion, and it's not just about finance-related administrations and organizations, the degree where we managed blockchain exterior to its digital finance origins the principal run through. Actually, the intermingling of blockchain and the IoT is on the plan for few groups, and there are existing usage, arrangements, and activities in a few territories and outside of IoT and finance domains as well. Blockchain at its midpoint is a cryptographically highly encrypted, carried record that considers into account the secure altercation of material between parties.

Conservative IoT tools rely on centralized engineering. Information is directed from a tool to the cloud where the information is controlled exploiting analytics and afterward directed back to the IoT tools. With billions of devices set to intersect with IoT systems in the coming years, this sort of centralized tool has constrained adaptableness, has exposed billions of pain points that trade to organize encryption, and will turn out to be unfathomably overpriced and restrained if outsider requires to recurrently check and corroborate every particular micro-scale altercation between devices (Fig. 4).

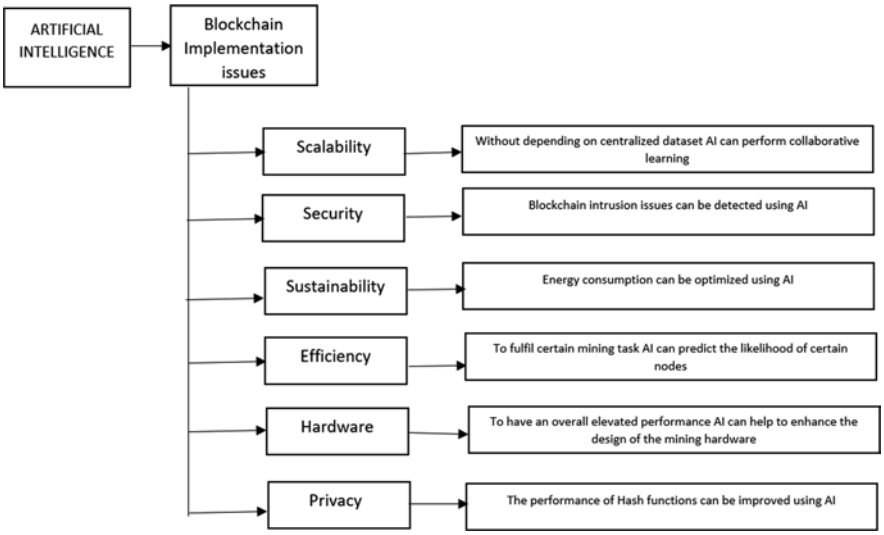


Fig. 4 A united approach of blockchain and AI

4.4 Certain Use Cases of Blockchain with IoT

Blockchain in combination with IoT can expand the traceability of the supply chain setup. IoT sensors, like temperature, motion, and GPS sensors, are allied to the vehicle to give information about the supply status. Data drawn from the sensors are stored in the blockchain by making it traceable, auditable, and transparent in the system.

Smart Homes
IoT devices permit home security system to be monitored digitally from the smartphone. But the centralized methodology for swapping information produced by IoT sensors has deficient ownership over information and security principles. By shifting the data obtained from IoT devices to the blockchain, the problem of security issues will be resolved.

Parking Solutions
A business organization named NetObjex has gotten up with an idea of smart parking solutions with IoT and blockchain. Using IoT sensors, it is easy to search for unoccupied parking space and pay the money automatically with crypto wallets. Regarding parking areas, IoT sensors can collect data, such as the amount of time the vehicle is parked and vehicle number, to get the associated wallet address. The information that is collected will be automatically stored in the blockchain, which prompts smart events to automate payments. A lot of businesses have started to research the potential of blockchain in IoT networks.

4.5 Challenges that IoT Overcomes Using Blockchain

Keen agreements in blockchain structures will permit devices to execute without harm and self-sufficiently by constructing considerations that are just never-ending source of exterior inevitabilities. It not only considers supplementary prominent robotization, adaptability, and less rate interactions (no interloper desired to administer interactions) but can also forestall misusage of data by individuals who want to exploit the material for their specific benefit. Information is communal over a decentralized, cryptographically encrypted structure, which means it is exceptionally tough to compromise system security.

Finally, by using the way of a centralized fabric, the vulnerability of an unsocial resolution of failure impairing a complete structure is an incontrovertible chance. A decentralized blockchain system moderates this risk with a large number of distinct pivots that move statistics on a distributed (p2p) proposition to keep the IoT system running seamlessly. To outline the advantages of blockchain and Internet of Things (IoT) combined, IBM gives the case of composite altercation paths and coordination, in which brilliant agreements can follow (and by means of blockchain innovation register) the whole thing that has occurred to singular things and bundles. The advantages are as follows: inventory streams, accountability, first-hand types of agreements, and quickness, to give some examples.

5 Blockchain Support During the Pandemic

COVID-19 pandemic resulted with thousands of casualties across the globe that resulted in government imposing emergency measures. The use of artificial intelligence, data science, and blockchain has become the need of the hour in almost every field.

The unprecedented times that COVID-19 pandemic has infected and killed thousands of people around the world have forced governments to implement emergency measures. Right now, almost the entire world is practicing social distancing and is placed under lockdown. Governments are using sophisticated expertise such as artificial intelligence, data science, and blockchain integration with such platforms, which have become the need of the hour. It is applied to control and manage the pandemic data dispersal and contributions and reprieve dispersal and further reactions in a rapid and translucent way devoid of the breach of customer information. Blockchain is being used by numerous governments across the globe for analyzing and probing medical data, healthcare IT systems at higher granularity, and sharing information.

Digital identity is a brilliant ulterior feature of the blockchain platform in defeating the novel COVID-19: it helps in building precision contact-tracing applications to allow anonymity. Several firms across the globe are alleged of influencing information for the duration of this pandemic; blockchain can bring trust, security, and

transparency to medical records. Blockchain-based comprehensive pandemic GPS can be used to trace the rapid binge of the novel coronavirus, the quantity of ill citizens, and the quantity of healthy citizens [32].

5.1 Ways in which Block Chain Can Be Used

1. Data Management
The current pandemic has created a lot of medical data which are to be stored and secured for future research purposes to provide data-driven solutions. In such a case, blockchain stands as a boon that supports in handling such medical records by maintaining its integrity, which can indirectly help data scientist for their data analysis process. As blockchain supports in automatized data collection as it is stored in ledgers, it indirectly helps in protecting data from unauthorized access and maintaining patient privacy. The data can be only made accessible for diagnosis and research in the vaccine discovery process.

2. Healthcare Surveillance
In order to have a decentralized access toward data, blockchain stands as the perfect solution as it does not depend on any central authority. This helps in sharing data with ease and security. Many organizations such as healthcare authority, test centers, morgues, and government agencies could contribute toward data ledger surveillance. The organizations could act as a node in the blockchain, and if the system reaches a threshold, a warning is alerted to all the nodes.

3. Spreading Awareness
Based on the permission access, blockchain ledges can be modified or changed only when parties making use of it give that access, as the ledgers are basically immutable. This makes sensitive data to be secured; it also supports tracking data back to its origin. Upon accessing such ledges, information like number of causalities and infected patients can be made public, which helps the government to implement preventive measures by creating awareness.

4. Tracking Infections
So as to process health data with higher precision among various departments, the medical data surveillance will increase transparency. Blockchain can support in this transparency, and this further can help scientists to track the virus origin efficiently.

5.2 All-Round Support of Blockchain to Fight the Pandemic

Apart from the above medical support, blockchain can also help in the following ways in the fight against the pandemic [33].

Insurance Claims
Due to the coronavirus outbreak, a lot of medical issues have happened so far to majority of people. Due to this, data records are imbalanced for many medical insurance organizations worldwide. Due to the rapid increase of coronavirus cases in the world, health management organizations are facing tremendous economical imbalance. In China, Xiang Hu Bao has started a financial organization named Ant Financial's Online Mutual Aid, which is blockchain-based tool whose functionality is to process numerous new COVID claims. Since the functionality is online, person-to-person contact is reduced, and every record is automatically stored in cloud databases.

Education
Due to this COVID-19 pandemic, the education system across the world has been disturbed as the students stay at home and study. Majority of educational institutions are making a decision to conduct online classes and online exams. Odem is a platform which is a blockchain-based platform providing free resources to educational institutions. Odem platform might not provide the same experience as traditional system, but it is trying its best to bridge the gap between students and learning during this tough situation.

Donation Tracking
During the tough times, there are people who come forward to donate some funds to the people who are in need. During this pandemic, the funds are released from sports, celebrities, business leaders, etc. HyperChain is a Hangzhou-based blockchain platform which created a donation tracking network to help donors look into where the funds are required. The HyperChain platform is genuine and transparent with which it received millions of dollars during this pandemic situation.

6 Economy Upliftment Using Blockchain

6.1 Blockchain, AI, and IoT Can Support to Handle the Economy for the Post-COVID Future

Before the industrial revolution, economic growth to a great extent was achieved by an increase in population. More people meant more mouths to feed, more bodies to dress, and extra workers who provided manual labor. The industrial revolution disrupted the market and has revolutionized the traditional production methods to a certain form of automation which allowed to produce more with and for the same amount of people. In the last 150 years, technology has enabled the economy to outgrow the rapid increase in population, and the worldwide growth in networked computing power has quicken up this process by miles. While economic growth is not congruent to welfare, the economy ought to be growing to allow governments to pay their debts and guarantee pensions for those who have worked hard in the past. Enter blockchain, AI, and IoT.

The effect of COVID-19 pandemic extends not only on our economy but also on our daily lives, which also makes it very hard to get back to the pre-pandemic life. Creating an impact on the bottom line, it has made business to reduce their operations and effected to bolster their development. This is principally factual and accurate for modernizations which condense human-to-human interaction, systematize methodologies, and increment throughput in the middle of socially distancing.

This COVID-19 pandemic is like a demon spreading rapidly, due to which the shortage in technology is looking into AI, IoT, and blockchain-like techniques to solve this problem at the earliest. Due to this pandemic, organizations, businesses, and several industries are facing numerous issues. They found what they are lacking of. Supplying resources, deploying resources, and taking actions and decisions wherever required are becoming hectic, and people are unable to control this due to the lack of infrastructure. Blockchain which has numerous advantages is under development for several years, which has been considered now for controlling this situation and making decisions using this technique. Blockchain, AI, and IoT, on their own, have the potential to change our daily lives. Combined however, they could revolutionize the world in less than two decades because of the promise they hold to let "things" contribute individually to our economy.

6.1.1 Artificial Intelligence

Predictions by eminent analysts say that "by 2030 AI-based devices will be able to contribute beyond massive $15.7 trillion to the global economy." Numerous amount of technical improvements like intellectual information processing and facial and speech recognition have grown beyond belief due to AI.

Since COVID-19, consumer behavior has drastically changed, with consumers being wary of everything, and it won't be a cake walk returning to the pre-pandemic norms. Patrons will buy huge quantity of merchandises and services virtually or digitally, and as the population increases day by day, work will be performed remotely or virtually, i.e., work from home (WFH). In the urge to get back to the new normal, companies are moving toward the post-COVID normalcy to escalate their economy; in this regard, artificial intelligence is aiding toward overcoming new challenges. AI will be particularly useful for those within retail and supply chain industries. Using advanced data analytics and machine learning, AI drives to help these organizations discover novel purchasing configurations and aid in delivering a holistic personalized experience to the online consumers.AI tools analyze humongous amounts of information to acquire core configurations, aid computer structures to take decisions, foretell human behavior, and identify objects, images, and human speech, in the midst of various additional things. The beauty of AI-based systems is they uninterruptedly acquire and acclimate with hasty changes in the database. These proficiencies will be exceptionally cherished as corporations antagonize and acclimate to the ensuing inventive customary once this pandemic subsides. AI will progressively subsidize a lot to the anticipation of buyers' behavior, which is highly capricious, and aid corporates to start up essential operational

logistics. Chatbots may be responsible for customer support 24/7, which is one of the "must-haves" throughout the lockdown.

6.1.2 Internet of Things

There were approximately 26 billion IoT devices in 2019, and statista.com expects their number will raise to a whooping and astounding 30.73 billion in 2020 and to mind-boggling 75.44 billion in 2025. The projected market value for an individual in the USA by 2030 is about $150 billions, with 15 IoT devices estimated.

6.1.3 Blockchain Technology

In our main global supply chains, the COVID-19 pandemic exposed a general lack of connectivity and data-sharing evident. Future sustainability would rely on making wired networks open, interoperable, and practical. If there were any remaining questions about the potential of blockchain systems to enhance market transparency that relies on the seamless integration of disparate networks, COVID-19 has all but wiped them off.

Since blockchain technologies are suitable exclusively for data authentication, protection, and sharing, they are perfect for multi-party, inter-organizational, and cross-border transaction management. It is not just the nimble startups who use blockchain tools to counter the virus. Business firms such as the World Health Organization, IBM, Oracle, Microsoft, and other tech firms, government interventions, and international health organizations are collaborating in developing the open data platform called MiPasa, focused on blockchain. The application developed by the organization blockchain firm HACERA aims to identify the COVID-19 carriers and infection hotspots worldwide quickly and accurately. MiPasa will exchange information securely between two people, hospitals, and agencies that will assist in public health research.

Blockchain is not going to leave this war as it is playing an integral part in aiding establishments and governments throughout the globe retort and react to the rapidly mutating COVID-19 virus, and at this time, it is being assimilated into healthcare and food delivery.

The Role of Decentralized Payment Systems

On the other hand, a decentralized payment system based on blockchain will play a vibrant role in combating the virus, as businesses will collect payment from cryptocurrencies since cashless payments wipe out any risk of contamination through liquid cash. Additionally, ultra-fast cryptocurrency payment methodologies support to assist cross-border transactions within seconds of time, permitting the transfer of funds via disseminated ledger machinery with the practice of various corresponding ledgers and handling nodes, which has the caliber to allay the dispute from a distinct point of failure.

Tokenization Can Help Countries Build the Economy After COVID-19
Tokenization is responsible for an exclusive opening to reestablish the world once the COVID-19 pandemic ends. The destruction triggered by the pandemic has had an immense and fatal impact in the world, which is one of the most horrible economic downturns in history, with massive unemployment rates around the world. Blockchain-based platforms have made tokenization promising, by empowering the detachment of assets in an insignificant conceivable way. Tokenization sanctions the person with a miniscule extent to finance and subsidize in constructing the economy.

Tackling the Supply Chain Failures
Blockchain tool helps to confront supply chain downfalls uncovered by the COVID-19 pandemic and also helps to enhance the economic rescue practice. According to the World Economic Forum (WEF), the coronavirus pandemic has laid a terrific burden on governments and business firms to sustain irrepressible supply chains. It additionally said that the contemporary pandemic accentuates the requisite for businesses and governments to mend the truthfulness and attribution of medication products and medical provisions, along with food, goods, manufacturing, and consumer products. The blockchain distribution toolkit is crucial for making elucidations that put effort for an assemble of actors, together with less significant performers who may not have admittance to the required assets to unravel the significance of blockchain technology.

7 The Blockchain Toolkit by the World Economic Forum

7.1 Providing the Ecosystem Value

Blockchain is most operational in systematizing cross-enterprise flow of work, which means aiding professional methodologies and sharing statistics throughout the network-to-network borders impeccably. On the other hand, undertaking the necessary ecological unit with a granted governance drapery outlines the parts and conducts of participants, how and what statistics and logistics will be shared among the participants, data proprietorship, admission, exit norms, and finances.

A disseminated ledger incorporates specific noteworthy remunerations comprising of reorganization, superior tractability and obviousness, inventive trajectory, unconventionality, and many more. Likewise, whichever new technology set out in a business's day-to-day setup, blockchain incorporates supplementary contemplations as well, like supervising which statistics is a right fit to be positioned in the setup and who catches to transcribe those statistics to the mutual series. Discerning over and done with such concerns primarily on, and organizing in view of that to cope with them, is vital to a mission's accomplishment [34].

Blockchain functionalities are dependent on peer-to-peer commitment by means of mutual archives which aid the altercation of statistics and supervision of professional practices throughout an ecological unit. It encourages alliance despite

sustaining unconventionality. By means of blockchain, any individual can mechanize the corporate methodologies and pick which statistics to be made accessible to particular applicants in an ecological unit. For instance, an establishment may not aspire for a patron to raise the value of enhancements made in protecting stock intensities as that would offer them exchanging control and condensing capacity to reprioritize efforts established on demand. Whereas blockchain can be responsible for that prominence, a system of government makes decision on which statistics to share and with whom – truly a tailored practice!

7.2 Digital Identity

Alongside the emerging intricate yard goods for supply chains, trustworthy distinctiveness of peers in the supplying grid is vibrant to proficient and active setups. A trustworthy personality can be seen from countless perspectives, together with corporal and ordinal ones. A digital distinctiveness is primary to construct trustworthiness and empathy in the midst of shareholders in an ecological unit. If shareholders do not have faith in the character of their peers, the information apprehended in the blockchain elucidation will be judged to be untrustworthy, and the complete ecological unit will be unable to find its efficacy. The blockchain and IoT tracing methodology comes together and advises all supply chain contributors, providing each prominence a grander share of the supply chain. The supply chain grows into a web of solid corporations, more willingly than an interrelated chain or a setup. Distinctiveness is decisive to this instance, as conviction in each of the actors will have emotional impact on the conviction and its legitimacy.

7.3 Data Protection

The seeming deficiency of switch above the information is one of the foremost obstacles in the embracement of blockchain that voluminous supply chain corporates face. With noble task scheduling and engagement, nevertheless, this concern can be alleviated to a greater possibility. Blockchain technology under no circumstances necessitates an establishment to divulge more information than it is contented with. On-chain statistics can also be coded so that it is only operational by authorized individuals. Thus, in the act of picking and setting out a blockchain elucidation, a supply chain establishment has the real tractability to guarantee that it provides data protection, resolves privacy issues, and addresses those of other supply chain companions.

- *Option 1*: Unrestricted or restricted blockchain with encoding. When sensitive evidence is deposited in its original form in the blockchain, it should be encoded. Decryption keys are then shared over one more protected network.

- *Option 2*: Unrestricted blockchain with facts cryptographically concealed but mathematically operational by themselves by means of techniques like ZKP and homomorphic encoding.
- *Option 3*: Restricted blockchain with indispensable authorizations and role-based admittance monitoring are satisfactory enough to afford necessary privacy. Facts can be documented as raw data.
- *Option 4*: Restricted blockchain is combined with an unrestricted blockchain to store the raw facts or forms, while the unrestricted blockchain only stocks hashes. The restricted blockchain is designed to offer requisite privacy.

7.4 Information Integrity

Integrity of knowledge is the property that all participants have the right, accurate, and useful data used in a solution. In the supply chain context, the word "information integrity" is used here in the wider sense omnipresently, referring not only to a resistance to accidental data alteration but also to the completeness, timeliness, and consistency of the data over its entire existence. Specifically, blockchain defends against data theft, which is permanent once it goes on the public ledger. When the data is entered and validated via the consensus process, blockchain technology offers good security against additional changes, since all users on the network can quickly detect those changes. Therefore, blockchain helps to create a higher degree of traceability and data auditability so that any data that was inaccurately entered prior to consensus can be traced back to their origin. Achieving information integrity within blockchain applications is generally composed of three requirements: integrity of data origin, oracle integrity, and integrity of digital twin.

Information Origin Integrity

A banal misconception is that using blockchain alone will guarantee the integrity of the data. However, although blockchains can largely prevent data breach, the undetected modification of data once it is confirmed on-chain, blockchains will only enforce this on the data provided. If the data is not reliable to begin with, then making it permanent by storing it on a blockchain does not offer much value – "garbage in, garbage out." Therefore, it is obvious that, in order to guarantee information integrity in a blockchain and supply chain solution, information consistency and reliability must be maintained from the roots, i.e., point of development to the point of use on the blockchain. This is called integrity of data sources. A lack of credibility of data origin would prevent the blockchain participants from drawing valuable conclusions from the blockchain data, as the data itself is incorrect. To maintain authenticated data integrity in a blockchain and supply chain approach, the authenticity and reliability of the data from the point of development to the point of use on the blockchain must be maintained.

Oracle Integrity
The point of submission in the blockchain is a banal point or stage where problems can occur. Since blockchains themselves cannot directly access real-world information such as shipment status, weather conditions, and product prices, they have to rely on third parties to request this information, typically referred to as oracles. The entity that submits the information (the oracle) is always the same entity that supplies the data (the source of the data or the creator of the data). Those oracles are trustworthy either way. Based on the environment in which the blockchain solution resides, a degree of caution must be taken to ensure the oracles have not corrupted or missed data prior to the blockchain submission. It is called the dignity of the oracle. A failure to attain oracle integrity leaves a system of blockchains susceptible to malicious manipulation and exploitation.

Digital Twin Integrity
In conclusion, this is basic for blockchain and gracefully fastens answers for genuine articles such as materials and items on the blockchain in a computerized structure, for example, a token. This advanced portrayal is alluded to as the real-time entity "digital twin." The thought is that valuable certifiable information about the article, for example, its character, current area, and different measurements, can be joined to this advanced twin so as to yield helpful bits of knowledge about the state of these items in reality and refreshed as environments transform. The conspicuous worries by means of this plan are whether the information connected to the advanced twin offers a precise and opportune perspective on the physical item or the connection concerning the physical article and digital twin may have been undermined. These contemplations by and large establish the assets of digital twin respectability. An absence of digital twin respectability will make the advanced twins never again be an exact portrayal of the real world, which can forestall the recognition of lost, taken, and fake products.

7.5 Cybersecurity

As they settle on innovation choices, pioneers nowadays are assaulted with consistent features about expensive venture hacks, ransomware, and taken client information. Along these lines, any new innovation usage must incorporate sufficient protections against such nightmare scenarios. Due to the rapid development of blockchain technology, there are a number of key confidentiality and privacy concerns which can be logical to the blockchain space viability. Blockchain arrangements don't stand all alone; for example, they require availability, clients, and sound business forms. Along these lines, the confidentiality and privacy of a blockchain are justifiably notorious with the confidentiality and privacy of diverse tools it is assimilated with [35].

Step 1: Defining Security Objectives
It is the establishment of the hazard evaluation all things considered, and it educates each after advance. Considering the plan of action which shall be bolstered by blockchain, which are the significant confidentiality and privacy destinations to cultivate? Will privacy be pretty much significant than accessibility? Should secrecy be a given? Likewise, such security highlights must be maintained by an all-encompassing arrangement. Which portion of the framework should safeguard information respectability excluding a blockchain framework?

Step 2: Performing the Threat Estimation
A threat estimation check enables the association to comprehend what the blockchain arrangement should be shielded from, running from human mishaps to regular disasters and intentional cyberattacks. Separating among dangers by sorting them as indicated by abilities and expectation is a decent method to quantify the potential for disturbance. For example, an administration office may have abilities yet no expectation to assault a specific blockchain. Hackers, paradoxically, might be keen on hurting the notoriety of a specific association yet come up short on the capacity to defeat assured confidentiality and privacy boundaries.

Step 3: Performing the Vulnerability Estimation
An assessment of vulnerability allows the project team to better understand the aspect of the blockchain solution that will be exposed to attackers and what weak points could lead to negative outcomes down the road. It is difficult to find vulnerabilities, and all companies will routinely perform penetration testing on all aspects of the blockchain applications that they implement. Especially, the testing of smart contracts needs to be taken care. Defining a methodology to secure smart contract code early on is crucial to reducing the vulnerabilities.

Step 4: Defining Risk Probabilities
Characterizing risk probabilities considers their prioritization. Dangers occur out of the convergence of vulnerabilities as characterized in the past stages. Place in order all the risks by deciding the probability of specific vulnerabilities converging with specific dangers, and if that occurs, decide the risk of the effect. A profoundly significant hazard that is probably not going to happen shall be overseen uniquely in contrast to some degree effective damage which is possibly going to take place normally. The matrix in Fig. 4 can be utilized to characterize the dangers related with blockchain usage arrangements.

Step 5: Deciding What To Do with Every Risk
- *Condensing the risk*. Managing the danger and additionally the helplessness legitimately to comprehend its effect. In blockchain, enclosing sway is maybe further testing than with different advances, and accentuation ought to likely be put on diminishing vulnerabilities and stopping dangers. This methodology provides the finest risk controller but is commonly expensive. It is finely prompted for maximum and basic dangers.

- *Accepting the risk*. Recognize the reality and financial plan to deal with. This methodology is finely exhorted from low to moderate dangers.
- *Avoiding the risk*. Again put effort on the methodology frameworks so as to wipe out the particular confidential challenges altogether. Doing this and large includes exchange offs and tolerating the evacuation of specific functionalities or arrangement clients.
- *Transfer the risk*. Include an outsider, for example, an insurance agency or an outer specialist organization, to address the risk.

8 Conclusion

Blockchain innovations offer incredible potential in numerous COVID-affected situations, particularly in the supply chain. Because of the interruption in ventures and the prioritization of critical costs, notwithstanding, blockchain will be constrained into a brief lull. Given its advantages as far as unwavering quality of the supply chain, straightforwardness over numerous utilization cases, and monitoring of products, nonetheless, blockchain ventures are relied upon to recoup once the pandemic seizes to exist.

References

1. J. P. Conley, Blockchain and the economics of crypto-tokens and initial coin offerings, in Vanderbilt University Department of Economics Working Papers 17-00008 (2017). Available online at: http://www.accessecon.com/Pubs/VUECON/VUECON-17-00008.pdf
2. J. Li, W. Mann, Initial coin offerings and platform building. Social Sci. Res. Network (SSRN) (2018). https://doi.org/10.2139/ssrn.3088726
3. L. Arnold, M. Brennecke, P. Camus, G. Fridgen, T. Guggenberger, S. Radszuwill, et al., Blockchain and initial coin offerings: Blockchain's implications for crowdfunding, in *Business Transformation Through Blockchain*, ed. by H. Treiblmaier, R. Beck, (Palgrave Macmillan, Cham, 2019), pp. 233–272. https://doi.org/10.1007/978-3-319-98911-2_8
4. S. Abeyratne, R. Monfared, Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **5**, 1–10 (2016). https://doi.org/10.15623/ijret.2016.0509001
5. F. Tian, An agri-food supply chain traceability system for China based on RFID & blockchain technology, in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, (IEEE, Kunming, 2016). https://doi.org/10.1109/ICSSSM.2016.7538424
6. T. Hepp, P. Wortner, A. Schönhals, B. Gipp, Securing physical assets on the blockchain: Linking a novel object identification concept with distributed ledgers, in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'18)*, (ACM, Munich, 2018), pp. 60–65. https://doi.org/10.1145/3211933.3211944
7. J.P. Cruz, Y. Kaji, N. Yanai, RBAC-SC: Role-based access control using smart contract. IEEE Access **6**, 12240–12251 (2018). https://doi.org/10.1109/ACCESS.2018.2812844
8. Swarm. Swarm – Serverless hosting incentivised peer-to-peer storage and content distribution (2019)

9. D. L. K. Chuen (ed.), *Handbook of Digital Currency*, 1st edn. (Elsevier, 2015). [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170
10. NRI, Survey on blockchain technologies and related services, Tech. Rep. (2015) [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/0531 01f.pdf
11. M. Ali, Trust-to-trust design of a new Internet. PhD thesis, Princeton University (2017)
12. E.B. Hamida, K.L. Brousmiche, H. Levard, E. Thea, Blockchain for enterprise: Overview, opportunities and challenges. ICWMC **2017**, 91 (2017)
13. M. Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly Media, Inc, Sebastopol, 2015)
14. T. Mori, Financial technology: Blockchain and securities settlement. J. Secur. Oper. Custody **8**(3), 208–227 (2016)
15. D. Tapscott, A. Tapscott, Realizing the potential of blockchain: A multi stakeholder approach to the stewardship of blockchain and cryptocurrencies. http://www3.weforum.org/docs/WEFRealizing Potential Blockchain.pdf. Accessed 06 Oct 2018
16. G.W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money, in *Banking Beyond Banks and Money*, (Springer, Cham, 2016), pp. 239–278
17. N. Badshah. Facebook to contact 87 million users affected by data breach (2018). https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach
18. Pilkington Mark, Blockchain Technology: Principles and Applications, Research Handbook on Digital Transformations, Social Science Research Network (2016)
19. S. Melanie, *Blockchain: Blueprint for a New Economy* (OReilly Publications, Sebastopol, 2015)
20. Xu et al., A taxonomy of blockchain-based systems for architecture design, in *2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, 3–7 April 2017*, (IEEE, 2017)
21. V. Buterin, On public and private blockchains 2015 [Online]. https://blog.ethereum.org/2015/08/07/on-public-andprivate-blockchains/
22. Zyskind et al., Decentralizing privacy: Using blockchain to protect personal data, in *2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA*, (IEEE, 2015). https://doi.org/10.1109/SPW.2015.27
23. M. Sharples, J. Domingue, The blockchain and kudos: A distributed system for educational record, reputation and reward, in *Adaptive and Adaptable Learning. ECTEL 2016. Lecture Notes in Computer Science*, ed. by K. Verbert, M. Sharples, T. Klobučar, vol. 9891, (Springer, Cham, 2016). https://doi.org/10.1007/978-3-319-45153-4_48
24. Peter Sestoft, Autonomous pension funds on the blockchain, IT University of Copenhagen, Dagstuhl seminar (2017)
25. X. Yue et al., 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
26. Xia et al., MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access **5**, 14757–14767 (2017). https://doi.org/10.1109/ACCESS.2017.2730843
27. W. Xin et al., On scaling and accelerating decentralized private blockchains, in *2017 IEEE 3rd International Conference on Big Data Security on Cloud*, (IEEE, 2017). https://doi.org/10.1109/BigDataSecurity.2017.25
28. P. Rimba, A.B. Tran, I. Weber, M. Staples, A. Ponomarev, X. Xu, Comparing blockchain and cloud services for business process execution, in *2017 IEEE International Conference on Software Architecture (ICSA)*, (IEEE, 2017), pp. 257–260. https://doi.org/10.1109/ICSA.2017.44
29. T. Supriya, K. Vrushali, Blockchain and its applications – A detailed survey (2017). Available: https://www.ijcaonline.org/archives/volume180/number3/aras-2017-ijca-915994.pdf
30. W. Roger, D. Christian, B. Conrad Scalable funding of blockchain micropayment channel networks (2017). Available: http://drops.dagstuhl.de/opus/volltexte/2017/7363/pdf/dagrep_v007_i003_p099_s17132.pdf

31. C. George, Bitcoin – A brief analysis of the advantages and disadvantages (2017). Available: http://www.globeco.ro/wpcontent/uploads/vol/split/vol_5_no_2/geo_2017_vol5_no2_art_008.pdf
32. https://www.forbes.com/sites/rachelwolfson/2018/11/20/diversifying-data-with-artificial-intelligence-and-blockchain-technology/#6b8aa9b34dad. Accessed 24 Dec 2018
33. https://blockchain.news/analysis/how-blockchain-technology-is-helping-to-fight-the-novel-covid-19-pandemic
34. V. Buterin, A next-generation smart contract and decentralized application platform, white paper (2014)
35. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008)

Securing Healthcare Information Using Blockchain Technology: A Deep Insight

R. Ganesan, T. Devi, S. Rakesh Kumar, and N. Gayathri

Abstract Today's world has turned its attention toward blockchain technology due to its vast characteristics and essential features, making it apt for securing healthcare information. Apart from healthcare industry, even finance industry makes use of blockchain technology. The attackers may try to hack the system to get the records of the patients to gain useful information. It can also be breached when data is shared across environments such as sharing of data as well as images. The paper addresses blockchain technology as well as issues related to information in healthcare along with the comparison of works, making a deep insight into the issues and solutions. The paper also provides a survey on existing solutions along with good research ideas for future researchers in the field. Finally, the advantages along with the disadvantages of the works available so far have been discussed.

Keywords Blockchain · Encryption · Privacy · Security

R. Ganesan (✉)
School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
e-mail: ganesan.r@vit.ac.in

T. Devi
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
e-mail: devit.sse@saveetha.com

S. Rakesh Kumar · N. Gayathri
School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
e-mail: s.rakeshkumar@galgotiasuniversity.edu.in; n.gayathri@galgotiasuniversity.edu.in

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_12

1 Introduction

Healthcare is an important area of research as it is mainly considered with human life and has become particularly important nowadays [1]. Computer systems have revolutionized the field by incorporating many changes, starting from automating the system to information sharing as well as collaborating the diagnosis process [2].

The advancement in the field of healthcare has increased the competitive spirit in the industry of pharmaceuticals [3]. As a result, the medical records can be managed in a better way for the benefit of both patients and physicians. The use of computers has made this management to work in an effective way. Data about patient is stored in the computer systems, which helps the patients to avail services related to healthcare in underdeveloped areas also. Several issues related to the data stored can also be of benefit to the community of people doing research on it. Protecting the patient data from being exposed to the outside world can also be taken into account while considering the issues related to it [4].

Protection of healthcare data can be provided using blockchain technology which helps to manage information sharing among patients as well as doctors [5]. The architecture of blockchain is decentralized, which helps mainly in protecting the data of patients, dealing with privacy as well as security. Log management and data auditing are yet another important key features [6]. Despite the several advantages of blockchain technology, it still suffers from certain limitations such as anonymous network features making data availability.

In the coming years, the pharmaceutical industry will try to incorporate blockchain technology for better growth. Several scenarios can make use of this technology because of its advantages [7]. Also, future research is focused on identifying the key use of blockchain technology in the area of healthcare. The survey identifies key points in blockchain technology and also points its usage in healthcare industry [8]. The paper makes a deep survey of all the healthcare-related problems along with the use of blockchain technology.

Section 2 deals with the motivation, Sect. 3 deals with the issues pertaining to the blockchain technology, and Sect. 4 concludes the paper.

2 Motivation of Blockchain

The use of blockchain technology in the healthcare field has revolutionized the entire industry [9]. The factors motivating the use of such new technology in the field of healthcare are discussed in detail.

Computers play a major role in the field of healthcare, thereby improving the entire field including managing the records of patients and identifying unique tools that help in monitoring of patients as well as other samples [10, 11]. Whether it is public or private, data related to patient is stored on a daily basis, making managing such huge data a challenge [12]. Big data came into rescue to handle huge amount

of data which had several applications [13]. With the help of computers, several processes can be performed in a successful manner for the process of automation in any field [14]. It can also help in the field of medicine by focusing on the improvement of money-related issues as well as quality of the systems.

2.1 Blockchain Technology in Healthcare

The origin of blockchain technology is from cryptocurrencies after which it had many applications including those in healthcare as well as in finance and several other sectors [15, 16]. Assets can be recorded using blockchain technology. In this technology, blocks are connected with the help of hash functions and also handle the grouping of transactions in a distributed manner [17, 18]. Also, one of the important factors to be noted is the emergence of cryptocurrencies that played a major role in the use of blockchain technology. Several other types of technologies have emerged based on this [19]. It took versions from 1.0 to 3.0 and so on. The first version of this technology is considered to be more important in case of property transfer [20, 21].

The final version with 3.0 is the technology that is currently in use and has many applications in fields such as healthcare and finance [22]. The features of blockchain technology are important to be known [23]. Also, several definitions for blockchain technology can also be found in literature.

2.2 Types

To reflect the behavior of the network, blockchain is further classified as the following types [24] (Fig. 1).

P_b_BLK (Public Blockchain)
Transparency is the important feature of such blockchain [25]. Transaction can be validated when the blockchain is published, and then all nodes can participate. There is no prior permission necessary for such tasks, and node identity in the network, as well as their support, is not revealed. One remarkable example for such blockchain is Bitcoin [26, 27].

P_r_BLK (Permissioned Blockchain)
Organizations own such blockchain, where the entry of nodes is restricted and also there is a control over the transactions [28]. Authentication comes hand in hand to rescue such situations, as privacy of nodes is an important factor to be considered here. One remarkable example for such blockchain is MultiChain [29].

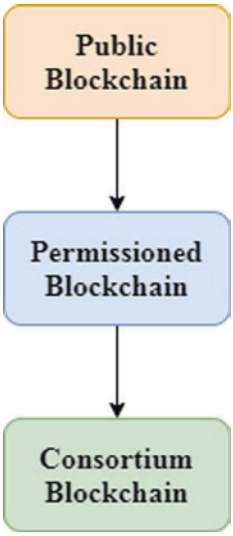


Fig. 1 Types of blockchain

C_n_BLK (Consortium Blockchain)
Like P_r_BLK, this is also controlled by organizations and also makes use of authentication in order to allow the nodes to take part in the network activities [30]. Every node has a sub-node to validate its work in case of transactions and also to help in creating a new block, thus ending the process [31].

2.3 Mining Process in Blockchain Technology

Mining algorithms in blockchain technology play a major role in validating the process [32]. Standard algorithms are employed for such purposes that frame the rules to be followed by the nodes [33]. The protocol which takes part in the transactions also notes that all nodes get corresponding responses, including the rules for transactions. Such situations help in deciding the insertion of the blocks. The protocols related to blockchain technology, specifically in relation with healthcare, are discussed below:

PoW – In case of proof of work [34], the mining process is one of the important steps in blockchain, where the nodes are in competition with one another to finish the puzzle related to cryptography. In such cases, one node that solves the puzzle becomes the first one to mine the chain and also helps in creating a new block [35]. Bitcoin is a well-known example where many exciting prices are offered to the winners.

PoS – In this proof of stake [36], based on the participant count, validation process is carried on the network. So, count of coins decides the block validation and also helps in the authentication of the nodes [37].

PBFT – Client and server play an important role in the validation process. Several steps are followed in order to validate [38, 39]:

(a) Request from client to server.
(b) Transmission to server nodes to identify the validity.
(c) Based on acceptance, notification of acceptance will be communicated to other nodes.
(d) Message is broadcasted by the nodes.
(e) Transaction sent by node is validated (Fig. 2).

One more protocol to note is smart contracts which can also be implemented with the help of Ethereum [40]. They are mainly focused in creation of rules that play an important role in validation of transactions.

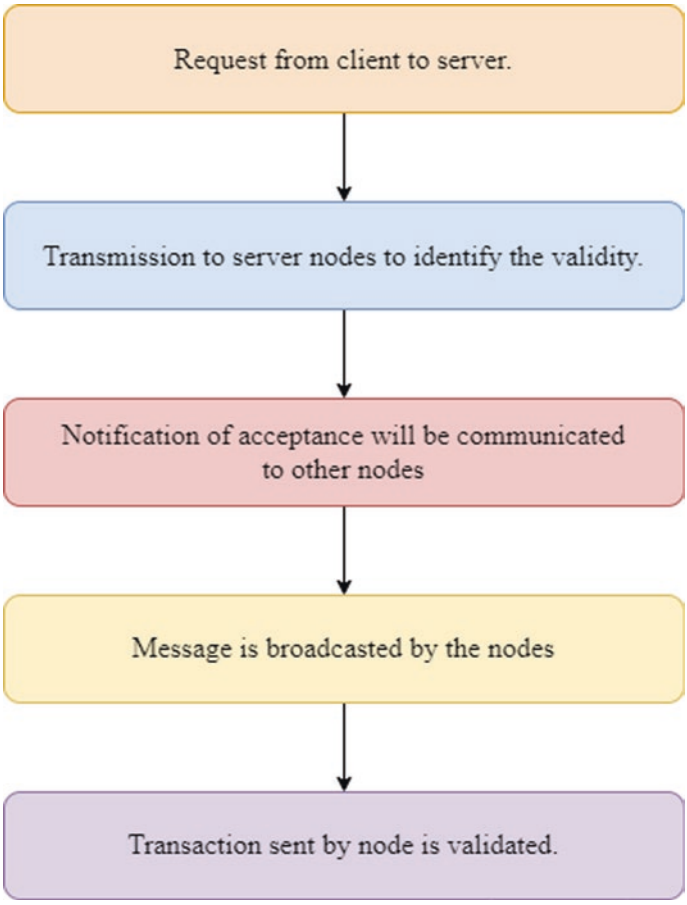


Fig. 2 Steps in validation of transaction

3 Issues in Blockchain Technology

The applications of blockchain include several sectors due to its advantages. Still, it suffers from certain limitations [41]. Many steps have been taken to overcome such issues as it stands as one of the main areas of research in today's world. Certain issues are discussed to know the facts available [42, 43].

While considering the number of nodes participating in the network, there arises the problem when the count increases [44]. This is an important feature to note in the case of healthcare, where throughput needs to be in higher rate [45]. The reason behind this is if the access is faster, the life of an individual can be saved, making throughput an important issue so far [43, 46].

Next come the issues related to latency. Validation time of a block can be as short as a few minutes [47, 48]. But this timeframe may be enough for the network to be hacked by the attackers. Due to the dynamic nature of systems, delays should always be avoided as it may endanger the life of a patient, making latency the next issue to be noted [49].

The attackers try to take control of the entire network at times, which may result in the failure of the healthcare systems. This also should be taken care of as security of data is very much important [50].

The process of validation requires more resources, which adversely affects the resources on other hand. In the case of healthcare, the devices used to monitor the patients are usually of higher cost. Consumption of resources is the next issue to be taken care of as the resources involved in blockchain have more cost for computation [51, 52].

In order to attract the patients, a programming interface is very much necessary as users need an easier interface to interact with. Also, the individual and technicians have less experience, necessitating the creation of an easy-to-use environment. This makes usability the next issue to be noted [53].

Validation process is centralized, but blockchain on the other hand is decentralized. Reliability of network gets affected and reduced also. If the main node is compromised, the data transferred to other nodes can also be hacked easily through several other attacks, thus making centralization as the next issue in healthcare industry [54].

Node privacy is the next important feature to be paid attention to. There are several rules and regulations related to node privacy.

3.1 Securing Healthcare Records Using Blockchain Technology

Compared to the previous medical records which were documents in physical appearance, now many healthcare sectors are working digitally to enhance their workload. Information is gathered in such industry from the records of patients, images related to those, as well as sensors.

Database helps in storing information about the patients, which seems to be sensitive as it stores confidential information. In order to secure such records, blockchain technology comes to rescue as it has several characteristics to secure the confidential information. This security can be achieved using cryptography in such systems [55, 56]. Several methods are available in the field of cryptography to secure sensitive information.

Along with security, privacy of data also needs to be given attention as records must be secure when transaction takes place. Privacy-related issues do exist in healthcare records such as privacy related to identity as well as transactions. The former privacy is related to disclosure of individual identity during the transaction, while the latter deals with preventing unauthorized access by users.

The records of patients contain confidential information related to their medical history. It also includes the details pertaining to registration of a patient as well as the transaction methods such as credit card or debit card details used by the patients. Several techniques have been analyzed in order to address such issues. Privacy model has been set up to address such issues also.

Various privacy techniques existed in literature, and the most important among them which grabbed the researchers' attention includes homomorphic encryption as well as zero-knowledge (zk) proofs. The Health Insurance Portability and Accountability Act (HIPPA) also concentrates on privacy of healthcare data. The highlights of the above act include sharing of data in such environment and identifying standards to protect information. The rules in the HIPPA include plans related to healthcare, provision related to healthcare, and associates in business [57].

Patient data must be protected in terms of reliability and security. Blockchain technology goes hand in hand along with the rules related to privacy to secure the information. Also, the HIPPA helps in restricting the access to the records of patients stored in database. Such barriers make the attackers impossible to access the confidential information of patients stored in hospital management systems, thereby protecting the patients' records [58].

ABE called as attribute-based encryption is one of the cryptographic techniques that makes use of attributes of data to encrypt the message along with access control over the information. Another model based on record sharing was also proposed to handle patient records with the help of Ethereum. It was mainly used to the rules related to blockchain along with file systems to handle data sharing. It also incorporated ABE techniques for encrypting data in order to secure the records. At the same time, the above technique suffers from the limitation of more expenditure spent on computation.

Repositories to store medical data also were utilized in huge numbers to provide privacy for such information. Such characteristics remove the worries of users from knowing about the breach of their sensitive information. Also, such security is being extended to the other areas such as big data. The table shows the details in clear (Table 1).

Even multimedia data can be handled by such systems using blockchain technology. Several authors have used different techniques to address the issues pertaining to the systems. Copyright issues can be handled by using watermark in order to

Table 1 Advantages and disadvantages of existing works

Problems in data	Advantages	Disadvantages
Record sharing	Interoperability of system	Key access prohibited
Security of records	ABE for data encryption	More complex
Privacy of records	Search in blockchain	Computation cost high

ensure data security. Another issue arises when records are being shared across environments. Proof-based works along with encryption techniques can be applied to overcome the problems created. With the help of blockchain technology, healthcare records can be secured in an effective manner.

4 Conclusion

Healthcare management system concentrates on storage of records containing the information related to patients. Several issues arise in storage of data online where blockchain technology comes to rescue. Our survey gives a deep insight into the issues related to healthcare information and also the works available in literature for solving the problems. Based on blockchain, the pros as well as cons of the existing methodologies were also discussed.

References

1. K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, M. Saadi, Big data security and privacy in healthcare: a Review. Procedia Comput. Sci. **113**, 73–80 (2017). https://doi.org/10.1016/j.procs.2017.08.292
2. A. Acar, H. Aksu, A.S. Uluagac, M. Conti, A survey on homomorphic encryption schemes: theory and implementation. ACM Comput. Surv. **51**(4), 35 (2018)
3. A.G. Modum.io, Whitepaper: Technology data integrity for supply chain operations, powered by blockchain (2017). Retrieved October 1, 2018 from: https://assets.modum.io/wp-content/uploads/2017/08/modum_whitepaper_0.9.pdf
4. A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, MediBchain: a blockchain based privacy preserving platform for healthcare data, in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, (Springer International Publishing, Cham, 2017), pp. 534–543. https://doi.org/10.1007/978-3-319-72395-2_49
5. A. Albeyatti, Medicalchain (2018). Retrieved September 30, 2018, from https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf [White paper]
6. J.P. Albrecht, How the GDPR will change the world. European Data Protection Law Rev. **2**(2016), 287 (2016)
7. Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J.A. Abedlla, K. Shuaib, Introducing blockchains for healthcare, in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, (IEEE, 2017), pp. 1–4. https://doi.org/10.1109/ICECTA.2017.8252043
8. A. Ali, F.A. Khan, Key agreement schemes in wireless body area networks: taxonomy and state-of-the-art. J. Med. Syst. **39**(10), 115 (2015). https://doi.org/10.1007/s10916-015-0272-9

9. 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**, 1 (2018). https://doi.org/10.1109/COMST.2018.2886932
10. S. Ogoh Alubo, Death for sale: a study of drug poisoning and deaths in Nigeria. Social Sci. Med. **38**(1), 97–103 (1994). https://doi.org/10.1016/0277-9536(94)90304-2
11. J. Alwen, J. Blocki, B. Harsha, Practical graphs for optimal side-channel resistant memory-hard functions, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, (2017). Retrieved September 20, 2018 from https://eprint.iacr.org/2017/443
12. J. Anderson, Securing, standardizing, and simplifying electronic health record audit logs through permissioned blockchain technology. Ph.D. Dissertation. Dartmouth College (2018). https://www.cs.dartmouth.edu/~trdata/reports/abstracts/TR2018-854/
13. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: using blockchain for medical data access and permission management, in *In 2016 2nd International Conference on Open and Big Data (OBD)*, (IEEE, 2016), pp. 25–30. https://doi.org/10.1109/OBD.2016.11
14. V. Balasubramanian, D.B. Hoang, T.A. Zia, Addressing the confidentiality and integrity of assistive care loop framework using wireless sensor networks, in *In 2011 21st International Conference on Systems Engineering*, (IEEE, 2011), pp. 416–421. https://doi.org/10.1109/ICSEng.2011.82
15. Ana Sofia de Oliveira Guedes Bastos, Quality of health information on acute myocardial infarction and stroke in the World Wide Web. Master's thesis. Universidade do Porto (2011)
16. L. Bell, W.J. Buchanan, J. Cameron, O. Lo, Applications of blockchain within healthcare. Blockchain in Healthcare Today **1**(2018), 1–7 (2018). https://doi.org/10.30953/bhty.v1.8
17. E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, V. Madars, Zerocash: Decentralized anonymous payments from bitcoin (extended version) (2014). Retrieved February 5, 2018 from http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf
18. J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in *IEEE Symposium on Security and Privacy (SP'07)*, (IEEE, 2007), pp. 321–334. https://doi.org/10.1109/SP.2007.11
19. D. Bhowmik, T. Feng, The multimedia blockchain: a distributed and tamper-proof media transaction framework, in *2017 22nd International Conference on Digital Signal Processing (DSP'17)*, (IEEE, 2017), pp. 1–5. https://doi.org/10.1109/ICDSP.2017.8096051
20. D. Bhowmik, A. Natu, T. Ishikawa, T. Feng, C. Abhayaratne, The Jpeg-Blockchain framework for glam services, in *2018 IEEE International Conference on Multimedia Expo Workshops (ICMEW'18)*, (IEEE, 2018), pp. 1–6. https://doi.org/10.1109/ICMEW.2018.8551519
21. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
22. T. Bocek, B.B. Rodrigues, T. Strasser, B. Stiller, Blockchains everywhere—A use-case of blockchains in the pharma supply-chain, in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM'17)*, (IEEE, 2017), pp. 772–777. https://doi.org/10.23919/INM.2017.7987376
23. V. Buterin, A next-generation smart contract and decentralized application platform (2014). Retrieved August 20, 2018 from https://github.com/ethereum/wiki/wiki/White-Paper
24. C. Cachin, Architecture of the hyperledger blockchain fabric (2016). Retrieved August 31, 2018 from https: //www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf
25. C. Cachin, M. Vukolic, Blockchain consensus protocols in the wild. CoRR abs/1707.01873 (2017), 1–24. arxiv:1707.01873 http://arxiv.org/abs/1707.01873
26. W. Cai, Z. Wang, J.B. Ernst, Z. Hong, C. Feng, V.C.M. Leung, Decentralized applications: The blockchain empowered software system. IEEE Access **6**(2018), 53019–53033 (2018). https://doi.org/10.1109/ACCESS.2018.2870644

27. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195
28. R. Campbell, Modum.io's temperature-tracking blockchain solution wins accolades at kickstarter accelerator (2016). https://bitcoinmagazine.com/articles/modum-io-s-tempurature-tracking-blockchainsolution-wins-accolades-at-kickstarter-accelerator-479162773/
29. M. Castro, B. Liskov, Practical byzantine fault tolerance, in *Proceedings of the T3rd Symposium on Operating Systems Design and Implementation (OSDI'99)*, (USENIX Association, Berkeley, CA, 1999), pp. 173–186. http://dl.acm.org/citation.cfm?id=296806.296824
30. S. Cha, J. Chen, C. Su, K. Yeh, A blockchain connected gateway for BLE-based devices in the Internet of Things. IEEE Access **6**(2018), 24639–24649 (2018). https://doi.org/10.1109/ACCESS.2018.2799942
31. K. Chatterjee, A.K. Goharshady, Y. Velner, Quantitative analysis of smart contracts, in *Programming Languages and Systems*, ed. by A. Ahmed, (Springer International Publishing, Cham, 2018), pp. 739–767
32. B. Chaudhry, J. Wang, S. Wu, M. Maglione, W. Mojica, E. Roth, S. Morton, P. Shekelle, Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Ann. Intern. Med. **144**(10), 742–752 (2006)
33. L. Chen, W.-K. Lee, C.-C. Chang, R.K.-K. Choo, Blockchain based searchable encryption for electronic health record sharing. Futur. Gener. Comput. Syst. **95**(2019), 420–429 (2019). https://doi.org/10.1016/j.future.2019.01.018
34. Clinicoin, Clinicoin—blockchain powered global wellness (2018). Retrieved February 5, 2019 from https://icorating.com/upload/whitepaper/pTpjzwFCNILrde22da7EQfxVpJZoDK-CoLx22yavq.pdf
35. L. Costa, B. Pinheiro, R. Araújo, A. Abelém, Compartilhamento seguro de arquivos de Saúde usando criptografia baseada em atributos e redes descentralizadas, in *Anais do XVIII Simpósio Brasileiro de Computação Aplicada a Saúde (SBCAS'18), Vol. 18. SBC, Natal, RN, Brazil*, (2018), pp. 1–12. http://portaldeconteudo.sbc.org.br/index.php/sbcas/article/view/3682
36. A.F. da Conceição, F.S.C. da Silva, V. Rocha, A. Locoro, J.M. Barguil, Electronic health records using blockchain technology, in *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain – SBRC 2018)*, vol. 1, (SBC, 2018), pp. 1–14. https://portaldeconteudo.sbc.org.br/index.php/wblockchain/article/view/2357
37. U.M. Dias et al, Predição da Função das Proteínas sem Alinhamentos Usando Máquinas de Vetor de Suporte. Master's thesis. Universidade Federal de Alagoas (2007).
38. T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. **30**(7), 1366–1385 (2018). https://doi.org/10.1109/TKDE.2017.2781227
39. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, F. Wang, Secure and trustable electronic medical records sharing using blockchain, in *AMIA Annual Symposium Proceedings*, (American Medical Informatics Association, 2017), p. 650
40. D. Dujak, D. Sajter, *Blockchain Applications in Supply Chain* (Springer International Publishing, Cham, 2018), pp. 21–46. https://doi.org/10.1007/978-3-319-91668-2_2
41. C. Dwork, A. Roth, The algorithmic foundations of differential privacy. Found. Trends Theor. Comput. Sci. **9**(3–4), 211–407 (2014). https://doi.org/10.1561/0400000042
42. R.G. Dyson, Strategic development and SWOT analysis at the University of Warwick. Eur. J. Oper. Res. **152**(3), 631–640 (2004). https://doi.org/10.1016/S0377-2217(03)00062-6
43. S.R. Kumar, N. Gayathri, S. Muthuramalingam, B. Balamurugan, C. Ramesh, M.K. Nallakaruppan, Medical big data mining and processing in e-healthcare, in *Internet of Things in Biomedical Engineering*, (Academic Press, London, 2019), pp. 323–339
44. W.O. Erhun, O.O. Babalola, M.O. Erhun, Drug regulation and control in Nigeria: the challenge of counterfeit drugs. J. Health Popul. Dev. Countries **4**(2), 23–34 (2001). http://www.nigeria-pharm.com/Library/Drug_regulation.pdf

45. J.A.T. Fairfield, Smart contracts, bitcoin bots, and consumer protection. Wash. & Lee L. Rev. **71**(2), 36 (2014). https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3/.
46. Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in blockchain system. J. Network Comput. Appl. **126**, 45–58 (2019). https://doi.org/10.1016/j.jnca.2018.10.020
47. Y. Ge, D.K. Ahn, U. Bhagyashree, H. Donald Gage, J. Jeffrey Carr, Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. JAMIA **20**(1), 157–163 (2013). https://doi.org/10.1136/amiajnl-2012-001146
48. J.P.P. Gonçalves, L.R. Batista, L.M. Carvalho, M.P. Oliveira, K.S. Moreira, M.T.D.S. Leite, Prontuário Eletrônico: Uma ferramenta que pode contribuir para a integração das Redes de Atenção à Saúde. Saúde em Debate **37**, 43–50 (2013). http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-11042013000100006
49. P. Gope, T. Hwang, BSN-Care: a secure IoT-based modern healthcare system using body sensor network. IEEE Sensors J. **16**(5), 1368–1376 (2016). https://doi.org/10.1109/JSEN.2015.2502401
50. G. Greenspan, MultiChain private blockchain, white paper (2015). Retrieved September 10, 2018 from http: //www.multichain.com/download/MultiChain-White-Paper.pdf
51. R. Guo, H. Shi, Q. Zhao, Z. Dong, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access **6**, 11676–11686 (2018). https://doi.org/10.1109/ACCESS.2018.2801266
52. P. Dhingra, N. Gayathri, S.R. Kumar, V. Singanamalla, C. Ramesh, B. Balamurugan, Internet of Things–based pharmaceutics data analysis, in *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*, (Academic Press, London, 2020), pp. 85–131
53. U. Gupta, Secure management of logs in internet of things. CoRR abs/1507.05085 (2015), 1–6. arxiv:1507.05085 http://arxiv.org/abs/1507.05085
54. J.D. Halamka, A. Lippman, A. Ekblaw, The potential for blockchain to transform electronic health records (2017). Retrieved September 30, 2018 from https://hbr.org/2017/03/the-potential-for-blockchain-to-transformelectronic-health-records
55. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain databases 2, in *Blockchain, Big Data and Machine Learning: Trends and Applications*, (2020), p. 97
56. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global, 2020), pp. 165–177
57. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, Boca Raton, 2020)
58. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, Boca Raton, 2020), pp. 1–23

Decentralized Healthcare Management System Using Blockchain to Secure Sensitive Medical Data for Users

N. Deepa, T. Devi, N. Gayathri, and S. Rakesh Kumar

Abstract Humans used machines that run manually to meet their needs. Nowadays, humans can interact with smart machines that perform tasks both manually and automatically, including work-related tasks. The growth of smart machines is increasing rapidly over a short period of time. Smart machines can work under certain protocols. The fundamental concept of smart machines is that they perform activities allocated to them. There are two types of smart machines: wired machines and wireless machines. Wired machines run their best; on the other hand, there are some issues with wireless machines. They failed to develop a permanent and private network, as well as provide data protection. Researchers consider this as a serious issue, so they partnered up with the industry sector and created an application to solve this issue. The application solution is "blockchain." Blockchain is a process of actually collecting and growing the record list that gets interconnected with the help of certain protocols of cryptography. Every block contains a hash that is generated by associating with the previous block using transition data with a timestamp. Blockchain provides the public, private, consortium, and hybrid blockchains a wide range of built-in features. The scope of the industry sector is that the application can be used for a variety of purposes, such as security, transactions, and capability. And also this sector can also lead to practical applications such as healthcare management system. Blockchain applications in the healthcare management system require record sharing with efficient data interoperability and authentication. After building this application, we can use it for fraud detection, verification, and identification among others. Before, all systems built in the healthcare system were well-

N. Deepa (✉) · T. Devi
Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India
e-mail: ndeepa.sse@saveetha.com; devit.sse@saveetha.com

N. Gayathri · S. Rakesh Kumar
School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
e-mail: n.gayathri@galgotiasuniversity.edu.in; s.rakeshkumar@galgotiasuniversity.edu.in

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_13

organized, but the problem was a lack of stringent authentication. The existing systems also focus on the healthcare system, but the problem is that there is no security for patient data as confidential medical records are moved from one hospital to another for specialized treatments. In this proposed system, we can build this application using blockchain with stringent authentication. By considering this problem, we can propose the ADS application. SADS stands for stringent authentication and decentralized storage using blockchain. Stringent authentication is the process of providing high security protocols to the network using cryptographic SHA-256 hash algorithm. This application can be implemented using Ethereum blockchain technology. Decentralized storage is utilized for blockchain. Decentralized storage is where breaking up of storage records takes place from one major server to multiple servers. This allows easy access to medical information and also helps to further research.

Keywords Smart machines · Blockchain · Cryptography · Healthcare system · Industry sector · Authentication · Ethereum blockchain technology · Decentralized storage

1 Introduction

Considering the context of people health, the United States started the World Health Organization to care about various issues related to people welfare. The WHO also serves as one of the members of the United Nations Development Programme. The organization started the revolution toward the fight against a transparent disease that takes a long time to recover from. At that point, the organization focused on healthcare management system (HCMS) which can be authenticated using blockchain.

1.1 HCMS

Healthcare management system is where storing patient records takes place, including personal and treatment details, which can only be accessed by authenticated users. In 1932, Father Moulinier proposed this scheme in the University of Chicago associated with a Catholic hospital. It is a 2-yeargraduate degree program, with the first year serving as a formal graduate and the second serving as an internship. Healthcare management is the duty of the health administrator who probably looks into balancing costs and also helps in recording hospital details. Specifically in North America, they offered a special bachelor's degree in human resources, which included healthcare administrators. In Nepal, healthcare management study is a new discipline.

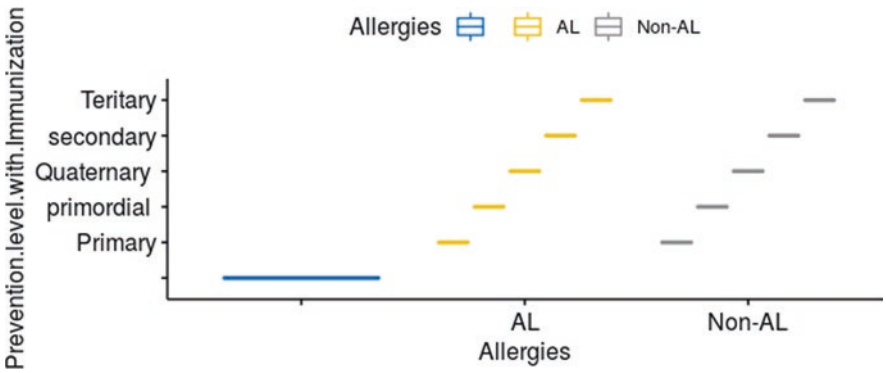


Fig. 1 Prevention level with immunization

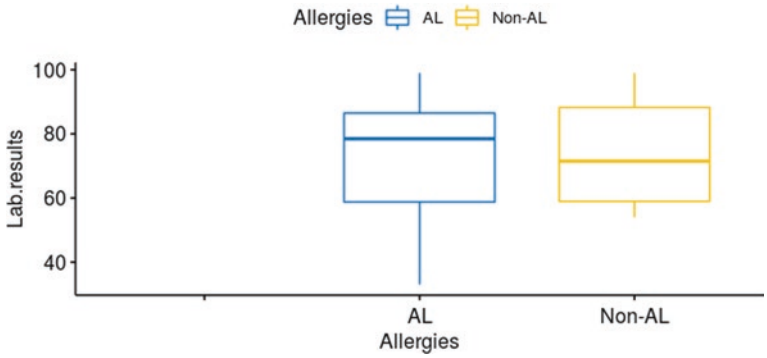


Fig. 2 Lab results of non-allergic and allergic patients

Prevention level with immunization is depicted clearly in Fig. 1 for both allergic and non-allergic patients. Lab results of non-allergic and allergic patients are shown in (Fig. 2).

Overall hospital records can be controlled by the hospital administrator, which can be categorized into two types: generalist and specialist. Generalists are in charge of managing and/or controlling the entire facility. On the other hand, specialists oversee and/or are responsible for the specialized departments such as finance and personal detail record, as well as business strategies.

1.2 Blockchain

Blockchain is the process of collecting and growing records that are connected using certain protocols and cryptography. Each block has a cryptographic function

associated with a transition data with a timestamp. Using this blockchain design, data can be modified in a safe manner.

The workflow of blockchain dealt with an issue of one timestamp being tampered with by another. In 1992, Bayer raised the issue of a blockchain that can be maintained in only one block. When this issue was brought to the attention of the public, they believed that the blockchain is not valid for design. After a long time, Satoshi Nakamoto described the overall process of the blockchain design in 2008. Improvisation of the blockchain design was done along with the hash functions by avoiding the timestamps between the blocks which maintained the list of records.

A blockchain is the process of collecting or growing the list of records called blocks, and each block is interlinked using cryptographic hash of the previous block with a transaction data and a timestamp. The main design resistant of the blockchain is the modification of data. The integration of multiple areas can be done by this block chain technology.

In the market, they are four types of block chain technologies:

1. Public blockchain
2. Private blockchain
3. Consortium blockchain
4. Hybrid blockchain

Public Blockchain: Public blockchain is the ledger distributed system with permissionless and non-restrictive mode. The main platforms in this blockchain are Bitcoin, Ethereum, and Litecoin.

Private Blockchain: Private blockchain is a closed network which is not completely distributed and decentralized.

Consortium Blockchain: Consortium blockchain is the semi-decentralized network which can be managed by more than one organization.

Hybrid Blockchain: Hybrid blockchain is the combination of private and public blockchain features, having permission and permissionless system.

A blockchain design can be altered with subsequent blocks processed by decentralization, distribution, and digital leader using the list of records in case of storage management. Today's digital token can be included with a cryptocurrency which is not only Bitcoin but also Ethereum, Litecoin, Monero, and so on. Stock markets, financial records, social networks, and healthcare systems all use blockchain to control their records and information. Blockchain doesn't deal with encryption where the data may be translucent. Figure.3 shows the application of various block chain technologies.Whenever confidential information, such as patient information and data related to disease, are considered in healthcare systems, it is important to be vigilant to prevent data loss or anonymous access, such as data pilfering, damaging, and so on [23, 24] (Fig. 3).

It requires tremendous expertise to secure data, and a block of data can be represented using a key to avoid fake data insertion and brute force attempts. The main purpose of implementing blockchain is to process data as a block using hashing techniques (dynamic and static), which allow for efficient linear and binary searches in patient records as well as replacement. Hashing as hs(x) has the same equal input

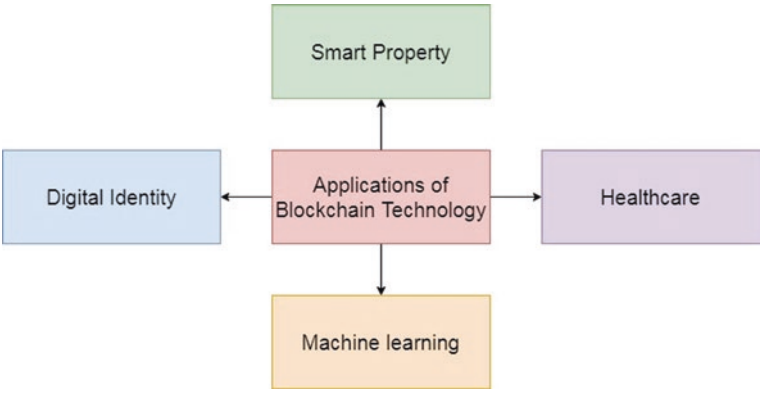
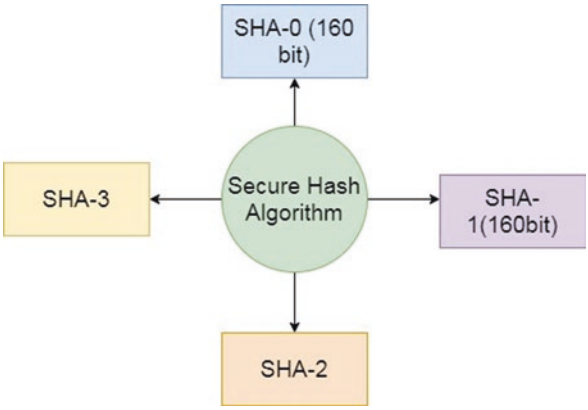


Fig. 3 Applications of blockchain technology

Fig. 4 Types of secure hash algorithm



and output, and different input can yield different results. Search engines such as Google and other social networks use the same hashing methods to secure passcode without storing the users' real password. Initially, the database stores the passcode in a hash format as h(pswd), ensuring that the input matches when the user enters the same as part of the verification process. To secure blocks of data, many hashing algorithms, such as SHA-1, SHA-2, MD4, and SHA-256 (Fig. 4), are utilized for encryption.

1.3 Cryptography

Data can be encrypted to ciphertext and decrypted to plaintext again.

Encryption
Encryption is the process of changing the plaintext into encrypted text by applying encrypted key. Encryption can take place on the sender side (Fig. 5).

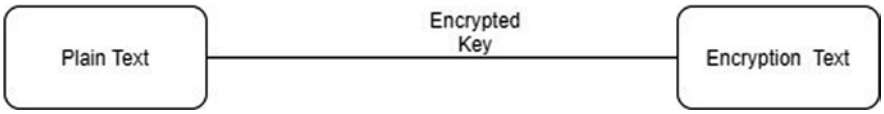


Fig. 5 Encryption of data

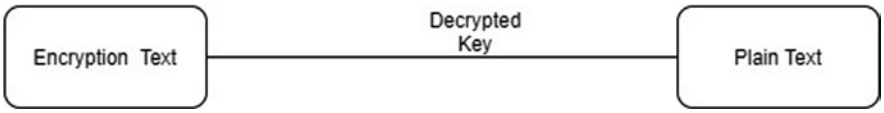


Fig. 6 Decryption of data

Table 1 Cryptographic algorithms

Algorithms	Blowfish	AES	3DES	DES
Key size	32-448	128,192,256	112 (or)118	64
Block size	64	128	64	64
Round	16	10,12,14	84	16
Structure	Feistel	Substitution permutation	Feistel	Feistel
Flexible	Yes	Yes	Yes	Yes

Decryption

Decryption is the process of changing the encrypted text into plaintext by applying the decrypted key. Decryption can take place on the receiver side (Fig. 6).

Table 1 shows various cryptographic algorithms and the parameters associated with them.

1.4 Hashing

Hash algorithm is the process of encrypting text from the source using hash function and then decrypting that hash text using the same hash function which can be used at the source side [25].

Encryption side (source): Plaintext can be transmitted from the source side to receiver side, at which point we can apply the hash function to the plaintext and convert it to hash text as seen in Fig. 7.

Decryption side (destination): The hash text is the input from the source side on the receiver side, at which point, we can apply the hash function to the hash text and convert it to plaintext as shown in Fig. 8.

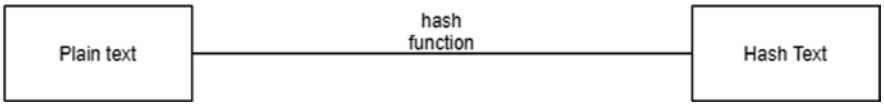


Fig. 7 Hashing in the source side

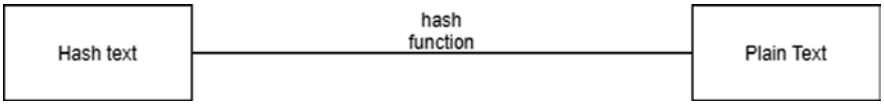


Fig. 8 Hashing in the receiver side

2 Related Work

Previously, all the existing systems for healthcare management were implemented by the database management system [1], following the database management protocols. Database management system is the process of storing, modifying, updating, deleting, and accessing the data. The details of the patient that contribute to the healthcare data can be stored in the database management system [2]. They store patient information and send it between their servers for patient treatments. The problem in such systems is they can't focus on the protection of patient records. At this juncture, the third party can easily access the patient records and can manipulate them for their own use. The patient records can be stored in the way of structured data.

Generally, data can divided into two types: structured data and unstructured data. Structured data is the process of storing the data in a structured manner such as files, documents, etc., and we can easily understand that data and can access any time easily. The unstructured data is the process of storing the data in an unstructured manner such as big data, etc., and we can understand easily but cannot access speedily.

In hospital administration, the administrator [3] maintains the overall information about the hospital records such as hospital patient details, finance records, business plans, and employee records. The responsibility of the administrator is to take care of the entry of new records, update the old records, and delete the unwanted records from the database storage. The administrator can send and receive the hospital records from multiple servers. While the transaction takes place, some list of records can be manipulated in the server network. An attacker can interrupt the network in the server because there is no protection for that transaction network as well as no authentication for the user. The existing works make use of cryptographic methods to safeguard their records. Cryptography is the process of performing the operations using cryptographic algorithms. In cryptography, encryption and decryption mainly play the major role.

Cloud-based electronic storage of medical data systems was proposed to deal with patient data which were private [4]. Remote monitoring of patient and storage of data online have aided progress in the field of medicine [5–7]. Proposed framework made use of sensors to collect medical data, and analysis was made on the data collected [8, 9]. Incorporating sensors in the medical equipment was also carried out [10, 27]. Access control function was also proposed based on blockchain technology that operated in a three-layer architecture [11–13]. Several systems focused on security and privacy, thereby enabling sharing of data across servers [14, 15]. IoT devices were utilized to collect data to be saves in the blockchain [16]. Electronic health records (EHR) were tested for integrity as well as confidentiality [17, 26]. Cryptocurrencies [18] such as Bitcoin became popular by blockchain technology, where blocks with cryptographic hash functions were used to maintain integrity of data [19–21].

2.1 Our Contribution

In every management system, transferring the list of records from one server to multiple servers for their jobs and benefits takes place. The hospital management systems consider the scenario where patient records can be transferred from one hospital server to another for better treatments and also research purposes. By considering this, we can ensure that the data transfer process is more stable. The main objective of the paper is to apply blockchain technology using cryptographic algorithms and to give more protection to the patient records. Also by giving authentication to the user, we can give protection to the sensitive information like categorical data, diagnostic treatment methods, and authorized parties who access information like specialized doctors, thereby protecting medical records [28, 29].

Authentication is the process of validation of the sensitive information or data of patients. In blockchain technology, the importance is focused on security and authentication process as the hospital healthcare division focuses on password security. The input data of patient's login password is converted into a digital signature (or) hash text or the so-called encrypted data by applying a security mechanism algorithm referred to as hash function of SHA-256. As we focus on SHA-256, the records are maintained in a highly protected manner so that the third party or hackers will not be able to view or access the sensitive information such as password, diagnosis, etc. However, the data on both client and server side are being accessed, where no data can be leaked and records are in a highly protected manner.

Organization of the Paper Section 2 describes the proposed system, Sect. 3 discusses the results, and Sect. 4 concludes the paper.

2.2 *Proposed System*

In hospital management system, the user can access all the records of the patient and hospital details. While transferring the records from one sever to another or transferring the records from one hospital administration to another, the third person can manipulate and misuse the records. By considering this problem, the proposed system uses blockchain technology. The system connects the website to the blockchain technology by applying the cryptographic algorithms to prevent third-party access by only using hash algorithm to authenticate valid users. Algorithm 1 shows the workflow of the proposed system and how the users are authenticated using valid username and password. By allowing authenticated users, the system prevents several attacks, and also Fig. 9 depicts the proposed system workflow.

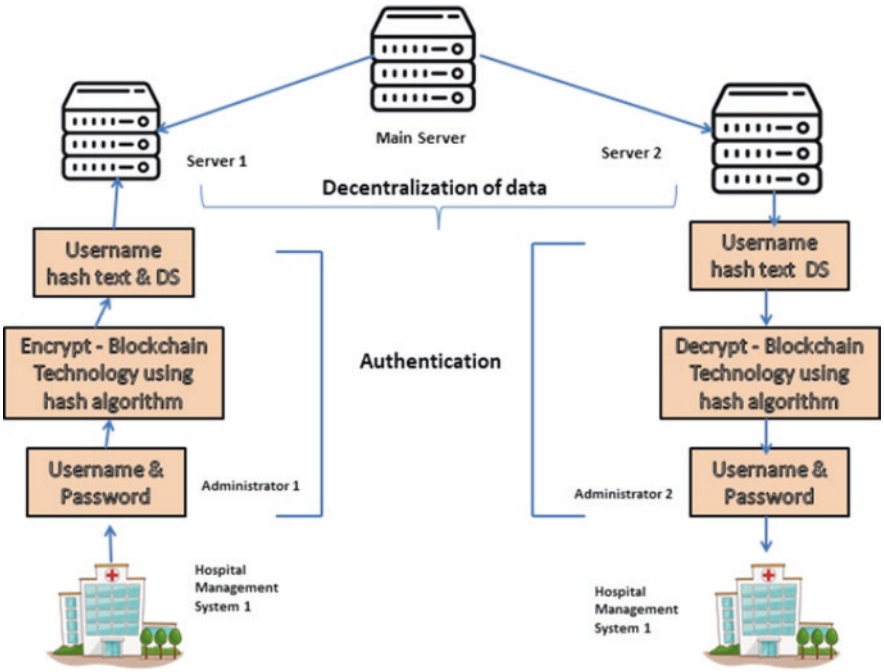


Fig. 9 Proposed system workflow

Algorithm 1

```
function aunthetication((user_data)
    if user 1 confirm username
    elseif user 1 confirm password
    Authenticate user 1 = hash (password)
    Generate hash function(H Hs)
 Pars encrypt ← hash_text (password)
 if user 2 confirm username
 elseif user 2 confirm password
    Authenticate user 2 = hash (password)
    Generate hash function(H Hs)
    Pars decrypt ← password (hash_text)
 if encrypt and decrypt are done over blockchain
 go to
 administration
 else
 goto (invalid user)
```

Algorithm 2: Encryption Algorithm

```
Function encryption (user_data)
 Username ← enter (input (username))
 Password ← enter (input (password))
 If user confirm username over blockchain technology
 Goto → encryption
 Generate hash function
 Encrypt_pars ← encrypt(password) + hash function
 Generate hash function
 DS ← encryptpass with hash_text
 Else
 Goto → Invalid user
```

Algorithm 3: Digital Signature (DS) Algorithm

```
Function DS(encrypt_pars confirm over blockchain technology
Goto → DS
Generate same hash function
DS ← encrypt_pars (hash_text)
Else
Goto → server problem
```

Algorithm 4: Decryption Algorithm

```
Function decryption (Ds_data)
    If Ds confirm over blockchain technology
    Goto → decryption
    Generate same hash function
    dencrypt_pars ← Ds(hash_text)
    Generate plain text
    Decrypt ← plain text_pars
    Else
    Goto → Invalid user
```

The algorithms for every phase are given in detail above to know the importance of the functions in the proposed system.

3 Results and Discussion

The implementation can be discussed in two phases: the first phase is creating an authentication login session without using blockchain technology, and the other phase is creating an authentication login session using blockchain technology.

A. *Authentication Without Using Blockchain Technology*

Authentication without using blockchain technology is the process of creating a login website using HTML while connecting with PHP and storing in database storage. HTML is the markup language which can be used to create webpages. PHP is the process of creating a connection between the HTML webpage and the database storage. And also it connects the tables in the database and stores values in it. For webpage database, we can use XAMPP tool. Creating a database using XAMPP and placing the database name "hospital records," we can store the username and password as shown in Fig. 10. The user can log in with the username and password, which are stored in the database.

B. *Authentication Using Blockchain Technology*

Authentication using blockchain technology is the process of creating a login website using HTML while connecting with PHP and storing in database storage, followed by applying the process of blockchain technology using hash algorithm. Finally, the database gets successfully inserted and authenticated with hash encryption (Fig. 11).

In case of authentication without blockchain, hospital management system uses normal algorithm. The username and password entered by the user is directly sent to the server without being protected.

On the other hand, in authentication with blockchain, hospital management system utilizes cryptographic algorithms. The user enters the username and password.

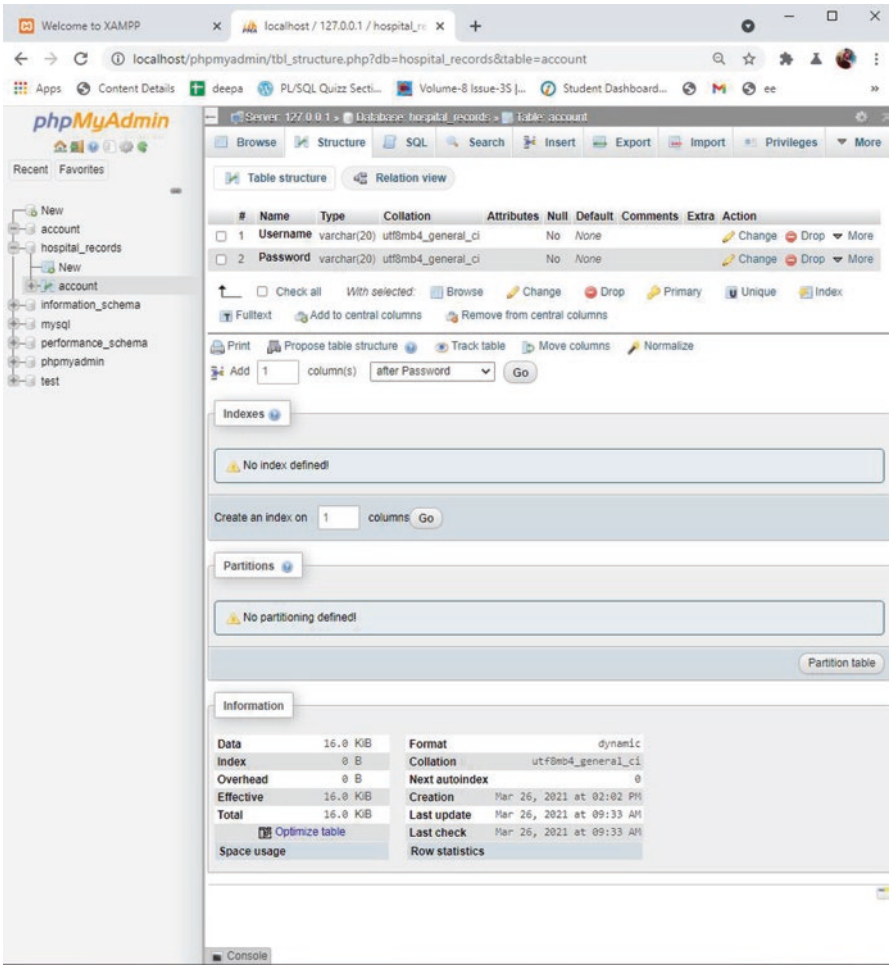


Fig. 10 Database insertion (without blockchain)

The password is being encrypted by hash function which generates the hashed text. The hashed text is sent to the server, and decryption is carried out using the same hash function, thereby depicting the validity of the user. Table 2 shows the encryption and decryption status of the password entered by several users.

Figure 12 depicts the comparison of various hash algorithms with SHA-256 algorithm used in blockchain technology for authenticating users. SHA-256 takes only lesser time to hash the passwords as compared with existing algorithms such as MD-5 and SHA-512 and so on.

Figure 13 shows the patient records on prevention level along with the password encryption level of several users logged in and authenticated successfully.

Figure 14 shows the usage of blockchain technology using SHA-256 in encrypting password of several users.

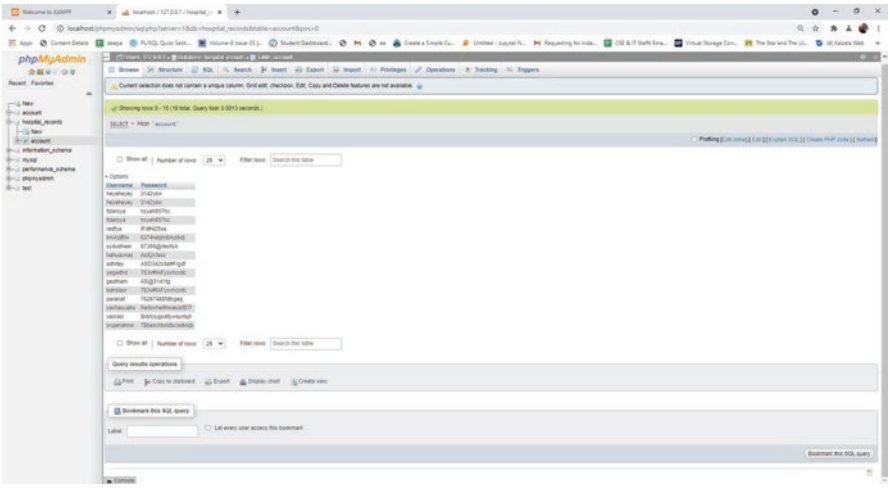


Fig. 11 Database insertion

Table 2 Encryption and decryption of password

Without blockchain			With blockchain				
Username	Password	Valid	Username	Password	Password encrypt	Password decrypt	Valid
Reddy123	1234@6	√	Reddy123	1234@6	$2y5105ma?y57	1234@6	√
Prasad143	Ha345	√	Prasad143	Ha345	$2y510593?!5785	Ha345	√
krish984	ABC543	√	krish984	ABC543	$3a?!57?5985?9	ABC543	x
bhuvan198	896CBA	x	bhuvan198	896CBA	$3b?1579598!?596	896CBA	x
vijay200	12@34	√	vijay200	12@34	$985?!65ba576c	12@34	√

The patient record details along with payment details are shown in Fig. 15. Details of patient information along with storage are shown in Fig. 16.

C. *Security Analysis*

The main requirement of security for any model includes confidentiality, integrity, and availability (CIA). User access by authorized people is possible only by proper storage of user identity in a database (Fig. 17). The proposed system helps in achieving confidentiality as the hospital servers store the identity of several users across the globe in a secure manner. Data transfer from source to destination cannot be modified in our proposed method due to the incorporation of SHA-256 hash algorithm for encrypting the passwords. Medical data is made available to both the users and medical practitioners [30].

Our proposed model cannot be prone to attack by the fraudulent people as the model provides robust security against the attacks.

1. DoS (Denial of Service) Attack: An attacker attacks the model as an authenticated user and also works in increasing network traffic. But using hash function

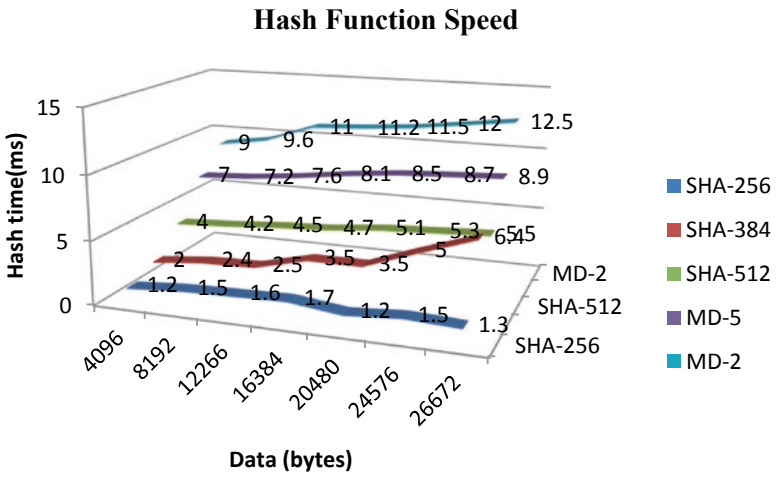


Fig. 12 Hash algorithm comparison

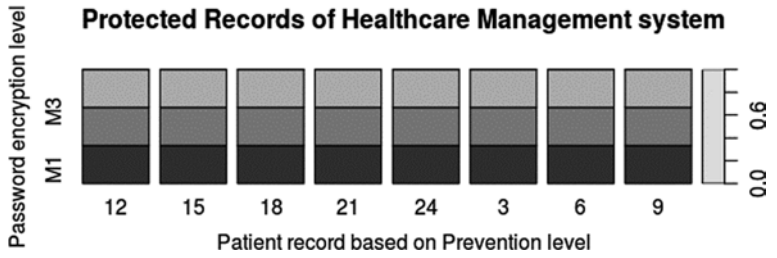


Fig. 13 Prevention level vs password encryption level

prevents the unauthorized users from accessing the medical data in the hospital management system.

2. Storage Attack: When the storage is being attacked, data can be modified in the server side. Blockchain technology using hash functions along with the usage of digital signature does not allow such attacks to take place in the proposed system.
3. Dropping Attack: Administrators in the proposed system are responsible for the storage of data on servers of system. Such scenario does not allow the control to be taken over by the attackers.

4 Conclusion

Human perception would never change rather than focusing on "health," although technologies are getting updated frequently in day-to-day life. By accepting the above statement, the WHO (World Health Organization) believes

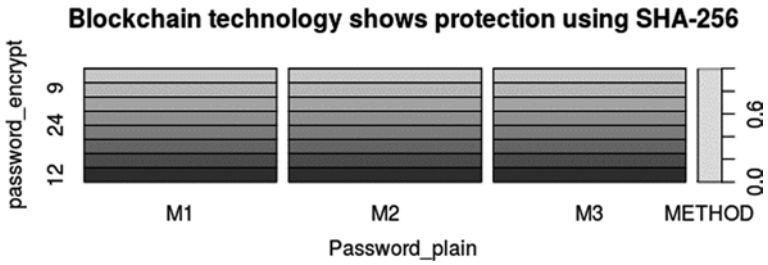


Fig. 14 Password encryption levels

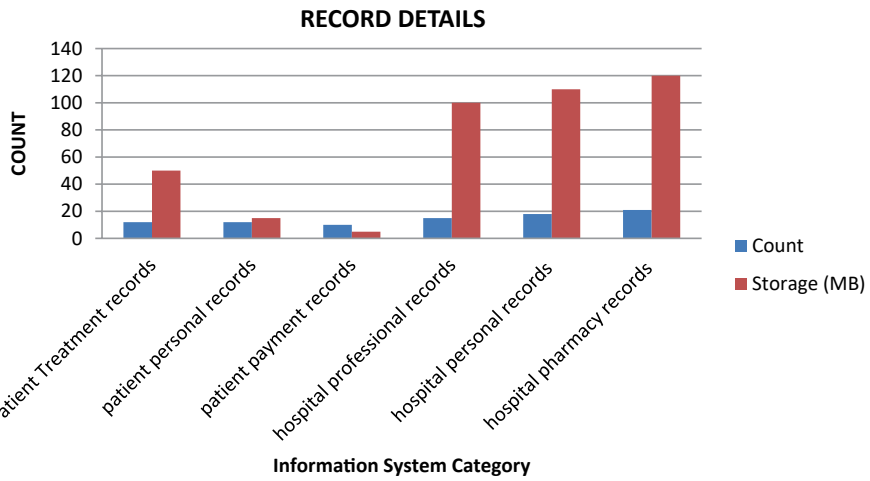


Fig. 15 Patient record details

the quote that "health is wealth." To be more clear, over the years, healthcare management systems played a vital role by implementing and involving management in various aspects, focusing on researches, laboratories, and so on related with healthcare. The main reason for storing and collecting patient records in hospital management is to follow further processes such as transferring the information to various hospitals for better treatment, among other reasons. In those situations, security and protection on records of patient are important. The main purpose of this paper is to show how the current blockchain technology protects patient records by applying cryptographic algorithms and how data can be decentralized while authentication is concentrated. Eventually, patient records can be transferred safely from one hospital server to another by granting valid user access only.

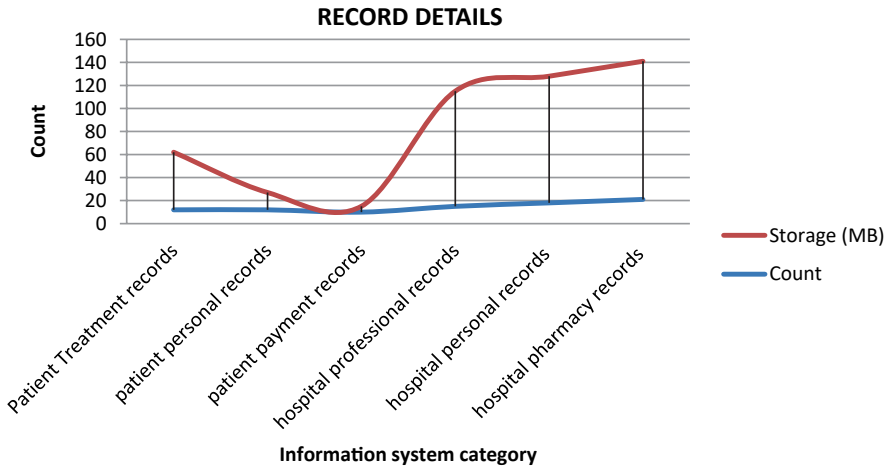


Fig. 16 Storage details of patients

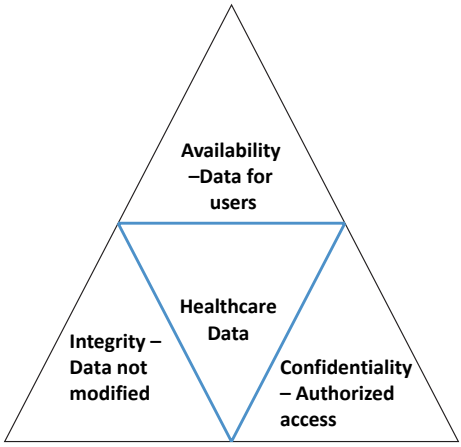


Fig. 17 CIA for proposed system

References

1. A. Ekblaw, A. Azaria, J.D. Halamka, A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data, in *IEEE Open & Big Data Conference*, (IEEE, 2016)
2. Fox News Health, *'Ransomware' Cyberattack Cripples Hospitals across England* (Associated Press, 2017)
3. A. Glaser, U.S. hospitals have been hit by the global ransomware attack – Recode (2017). https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-ushackers-nsa-hospitals
4. O. Gul, M. Al-Qutayri, C.Y. Yeun, Framework of a national level electronic health record system, in *2012 International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, (IEEE, 2012)

5. E. Hendrick, B. Schooley, C. Gao, CloudHealth: Developing a reliable cloud platform for healthcare applications, in *IEEE 10th Consumer Communications and Networking Conference (CCNC)*, (MediBchain, 2013), p. 543
6. S. Kiyomoto, M.S. Rahman, A. Basu, On blockchain-based anonymized dataset distribution platform, in *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, (IEEE, 2017)
7. L.A. Linn, M.B. Koo, Blockchain for health data and its potential use in health it and health care related research. healthit.gov (2016)
8. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system (2008)
9. M.R. Patra, R.K. Das, R.P. Padhy, CRHIS: Cloud based rural healthcare information system, in *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance*, (2012)
10. S. Raval, Decentralized applications: harnessing bitcoin's blockchain technology (2016)
11. C.O. Rolim, F.L. Koch, C.B. Westphall, A cloud computing solution for patient's data collection in health care institutions, in *International Conference on eHealth, Telemedicine, and Social Medicine*, (2010)
12. M. Simic, G. Sladic, B. Milosavljević, et al., A case study IoT and blockchain powered healthcare (2017)
13. M. Swan, Blockchain: blueprint for a new economy (2015)
14. X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **40**(10), 218 (2016). https://doi.org/10.1007/s10916-016-0574-6. ISSN 1573-689X
15. Y. Zhang, M. Qiu, C.W. Tsai, M.M. Hassan, A. Alamri, Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. **11**(1), 88–95 (2017). https://doi.org/10.1109/JSYST.2015.2460747. ISSN 1932-8184
16. A. Al Omar, M.S. Rahman, A. Basu, S. Kiyomoto, MediBchain: A blockchain based privacy preserving platform for healthcare data. Lect. Notes Comput. Sci **10658**, 534–543 (2017). https://doi.org/10.1007/978-3-319-72395-2_49.
17. A. Al Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, M.S. Rahman, Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Futur. Gener. Comput. Syst. **95**, 511–521 (2019)
18. F.A. Khan, M. Asif, A. Ahmad, M. Alharbi, H. Aljuaid, Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustainable Cities Soc. **55**, 102018 (2020)
19. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (BN Publishing, La Vergne, 2008)
20. L. Malina, J. Hajny, P. Dzurenda, S. Ricci, Lightweight ring signatures for decentralized privacy-preserving transactions, in *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, Porto, Portugal, 26–28 July 2018*, (2018), pp. 526–531
21. M. Mettler, Blockchain technology in healthcare: The revolution starts here, in *Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016*, (2016)
22. A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017*, (IEEE, 2017), pp. 618–623
23. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
24. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency, in *Cryptocurrencies and Blockchain Technology Applications*, (2020), pp. 181–195

25. S.R. Kumar, N. Gayathri, S. Muthuramalingam, B. Balamurugan, C. Ramesh, M.K. Nallakaruppan, Medical big data mining and processing in e-healthcare, in *Internet of Things in Biomedical Engineering*, (Academic Press, Amsterdam, 2019), pp. 323–339
26. P. Dhingra, N. Gayathri, S.R. Kumar, V. Singanamalla, C. Ramesh, B. Balamurugan, Internet of things–based pharmaceutics data analysis, in *Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*, (Academic Press, Amsterdam, 2020), pp. 85–131
27. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain databases 2, in *Blockchain, Big Data and Machine Learning: Trends and Applications*, (2020), p. 97
28. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global, 2020), pp. 165–177
29. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications* (CRC Press, Boca Raton, 2020)
30. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, Boca Raton, 2020), pp. 1–23

Imminent Threat with Authentication Methods for AI Data Using Blockchain Security

Vijaya Krishna Sonthi, S. Nagarajan, M. V. B. Murali Krishna M, Koppisetti Giridhar, V. Lakshmi Lalitha, and V. Murali Mohan

Abstract Since the announcement of Satoshi Nakamoto's Bitcoin policy document in 2008, blockchain has become one of the most widely discussed techniques for implementing safety storage and processing through decentralized, approved, peer-to-peer networks. This study described peer-reviewed literature, which uses cryptocurrency for cybersecurity purposes and offers a comprehensive overview of the most commonly used application areas of blockchains. This main forward-looking study further illuminates the possible directions for science, education, and practice on blockchain and cyberprotection, such as IoT blockchain security, as well as the need for data analysis of blockchain safe data. Analyses of this data increase the value of the latest machine learning (ML) technologies. There is a logical quantity of data required by ML for correct decisions. Data reliability and sharing in ML are very critical for improving the accuracy of performance. The combination of these two technologies will yield extremely accurate results (ML and BT). In this paper, we present a detailed review of ML adoption to make mobile platforms based on BT more resilient against attacks. Examples of such support systems as support vector machines (SVM) and bagging and deep learning (DL) algorithms can be used to evaluate attacks on a blockchain network, including convolutional neural network (CNN) and long short-term memory (LSTM). Actually, various traditional ML techniques are available. Furthermore, we include the use of both technologies in a variety of smart applications, including UAV, Smart Grid (SG), healthcare, and

V. K. Sonthi (✉) · V. L. Lalitha · V. M. Mohan
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
e-mail: svijayakrishna@kluniversity.in; vlakshmilalitha@kluniversity.in; muralimohan310@kluniversity.in

S. Nagarajan
Department of CSE, FEAT, Annamalai University, Chidambaram, Tamil Nadu, India

M. V. B. Murali Krishna M · K. Giridhar
Department of Computer Science and Engineering, Aditya College of Engineering, Surampalem, Andhra Pradesh, India

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_14

smart towns and cities. Future technological issues and concerns are also debated. Finally, we discuss the study model with a thesis.

Keywords Blockchain · Machine learning · Smart Grid · Data security and privacy · Data analytics · Smart applications

1 Introduction

Blockchain technology, as a distributed ledger of physical and financial resources, allows for trusted payments among unauthenticated network participants. Different blockchain networks, such as Ethereum and Hyperledger Fabric, have emerged through public and private availability outside traditional digital currencies and electronic token systems since the launch of the first Bitcoin blockchain. Multiple industries trying to adapt the core principles to existing processes have recognized the importance of a trustless, decentralized ledger which really carries traditional non-repudiation. For several business fields, such as finance, logistics, the pharmaceutical industry, smart contracts, and perhaps, most notably, cybersecurity, the specific properties of blockchain technology make its use an attractive concept in the context of this paper. The drastic shifts in production and distribution, including globalization and outsourcing, are the result of the higher degree of sophistication. As a consequence, various parts of global supply chains are operated by independent companies. By using local information such as cost structures, profit margins, and estimates, each organization in the supply chain establishes operational and strategic targets to optimize its very own profit. While advances in information technology allow businesses to gather, store, and exchange information, because of competing incentives, companies may be reluctant to do so. Trying to align rewards increases the profits of companies and sustains any use of information technology. The motivation concerns with a large risk imbalance, such as capability risk, need to be fixed. The effect of resource risk is more serious for a decentralized supply chain than for a vertically integrated supply chain because of the imbalance. We recommend a blockchain-based approach to resolve the double-marginalization issue in order to solve these problems [1].

2 Prioritize Vulnerabilities: From Identification

Discounting the value of incident prevention is standard. The sheer amount of vulnerabilities in their own organizations can be underestimated by executives. Additional risks that may emerge from acquisitions of many other companies may not be considered. These individuals could get some sobering facts, especially in light of market enforcement regulations, such as with the General Data Protection

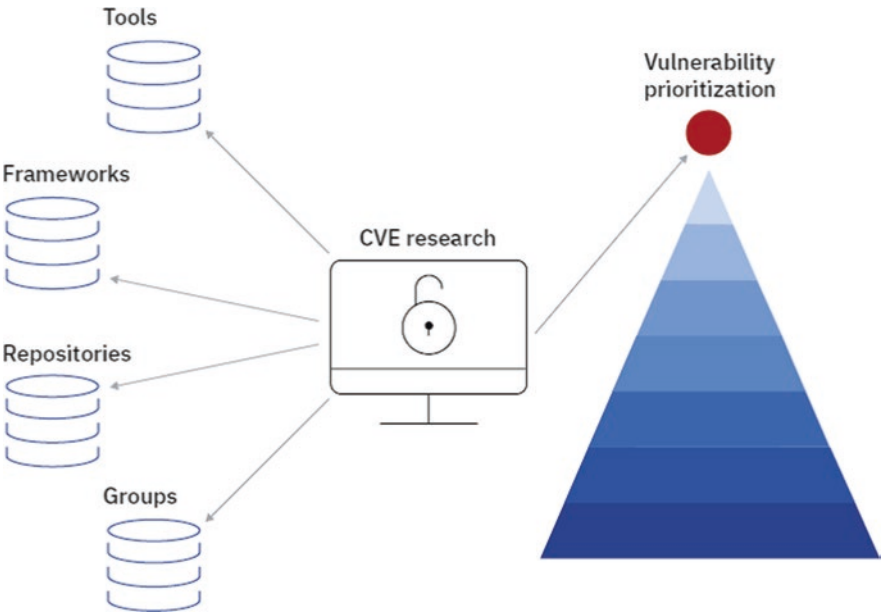


Fig. 1 An armed intruder insecurity rating approach is intended to offer a simple impression of containment

Regulation (GDPR). Personally curated data can also easily become outdated. It could take 3–5 full working days to complete the development of a database to rank vulnerabilities as shown in Fig. 1. New bugs are likely to appear by the time your spreadsheet is completed and may be ignored. Other factor to consider is indeed a lack of knowledge. Sometimes, business leaders feel that they are quick to fix when bugs are identified. As such, instead of seasoned data scientists, workers who lack updates and patch skills and training may obtain the assignments. When they are discovered, these novice workers are also not prepared to repair bugs [2].

Despite these conditions, several companies are presented with a long list of vulnerabilities that are not properly addressed. Organizations need to adopt a risk management program to further strengthen their defense capabilities [3, 4].

2.1 Identifying Flaws

Focusing on improving the most important vulnerabilities based on property value and cyberwarfare

Fixing after a manageable mitigation phase

The most risk-elevating vulnerabilities

The Popular Vulnerability Point System annotates each CVE identification using the CVSS. Based on an average, this economy standard is being used internationally to rate the seriousness and risk with CVE. A quantitative radiological rating is generated by the CVSS depending on multiple factors, along with the following:

1. Form of assault
2. Degree of access required
3. Sophistication levels [5]

3 Vulnerabilities and the Management of Remediation

Where a third-party remediation manager uses the "work increase" of hourly staff, the employees may use customer-provided or purchased vulnerability scanning from a supplier. The remedial service provider then communicates with the scanners used by ticketing or table customers. It is not likely that this strategy would yield results, as scanners might not be able to detect "not-yet-known" vulnerabilities that are not designed to defend against hacker thought and motives [6].

Companies must view vulnerability management as a multistage process, not a single process.

3.1 Scanning Efforts

A successful programmer, focused on a sheer number of existing and emerging vulnerabilities, will focus the institution's attention on the most high-risk vulnerabilities continuously.

One significant issue in remediating vulnerability is that corporations typically need not invest time and money on manufacturing [7].

Attackers could only initiate attacks on the infrastructure in a bitcoin system if an attacker controls 51% or more of the nodes. Because most nodes are run by genuine network nodes, attacks can be conducted very differently, and the block information in the blockchain is therefore credible.

Participants in the Bitcoin system pledge their privacy. By purchasing the longest working load-proof chain, participants can willfully leave or reenter the Bitcoin scheme to access transaction details while leaving the system [8].

4 Attack Model

4.1 Semi-Honest Model

Half-honest respondents in this model are also known as passive attackers. A semi-honest partner shall not withdraw from the deal nor interferes with the outcome of the protocol, in full compliance with the implementation of the contract during intra-computation. He or she is able to maintain.

Some intermediate outcomes in implementing the agreement attempt, through these intermediate outcomes, to evaluate and extract input data from other participants [9].

4.2 Malicious Model

Malicious assailants are also active model attackers. A malicious attacker can not obey the procedure of the protocol, interrupt the protocol operations, and concur with intermediate results or amend the contract with other parties as shown in Fig. 2.

5 Encryption of Authentication and Connection

CSE is focused on the intimacy of the user. If two people have much more mutual friends in society, there is a more intimate contact for both users. Thus, we measure intimacy by measuring two follow-up users. However, in the social network world, to prevent other users from miscellaneously entering user information to identify social circles, a user on two sides may confirm their identification before the communication process. In this sense, a user would have to know the personal information of other users. Consequently, we must authenticate the user's identity in case a malicious user gets the user connection inappropriate and infer the user's wishes and desires until a client receives details from other user relationship. Encryption of authentication is shown in Fig. 3 [10].

5.1 Hashing Blockchain

Since this is the first block in a sequence, it does not contain the pointer. At the same time, there is potential for a final block to exist in the blockchain database with no pointer.

Blockchain infrastructure can be useful for companies and businesses**.**

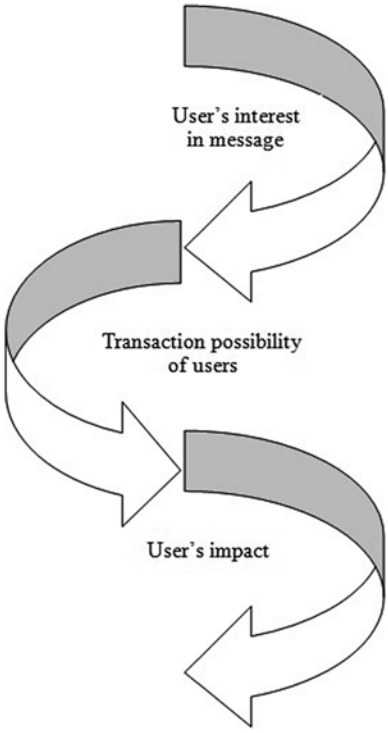


Fig. 2 Models for malicious attack

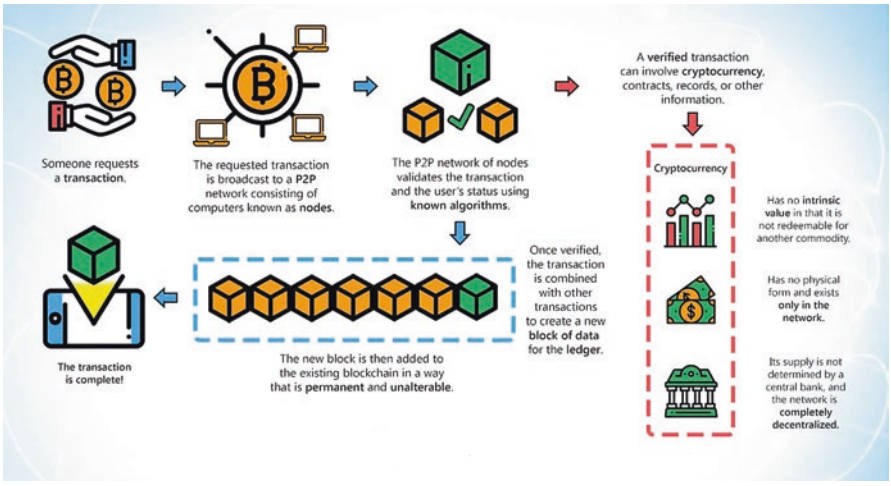


Fig. 3 Encryption of authentication

Reducing the cost of storing data can also be achieved by keeping data secure from cyber criminals and corrupt intentions [11].

History of Data: Inside a blockchain structure, you can check the history of any transaction at any time. A centralized database is more like a snapshot of information at a single point in time.

Data is maintained and controlled by the blockchain. Data is difficult to tamper with. Verification of records takes time since it happens in each individual network rather than in a compound mechanism (Fig. 3). That means we compromise output speed but instead have high protection and validity [12].

Blockchain systems fall into three groups.

5.2 Blockchain Technology Architecture: Public

A public blockchain design ensures data and access is open to anyone who is willing to participate (e.g., Bitcoin, Ethereum, and Litecoin blockchain systems) [13, 14].

5.3 Blockchain Architecture

In private device architecture, the user is only approved by a certain entity or has been given permission by a particular user.

5.4 Consortium Architecture

The blockchain can involve several organizations. In a consortium, procedures are regulated by the preliminary allocated users (Table 1).

Table 1 A detailed comparison among these three blockchain systems

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Designated set of nodes	Within one organization
Read permission	Public	Public or restricted	Public or restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Short	High	High
Centralization	No	Partial	Yes
Consensus process	Agreementless	Needs agreement	Needs agreement

Each block stores a combination of digital currencies and many records. For instance, the block keeps records of the transferor, recipients, and amount of money in Bitcoin blockchain.

The same way, a hash is a unique identifier (long record consisting of some digits and letters). The algorithm generates each block hash (SHA-256). This then allows simpler recognition of each block in a blockchain structure. If a block is mined, a hash is automatically formed, while any changes made in a block result in updating the hash. Hashes help evaluate any changes made to a block [15].

This is the final element of the preceding block hash. This provides protection and helps to deter security breaches. In this way, 45 and 46 are related. The very first block is unique because all other blocks originate from this block of origin.

Any corrupt attempts will guarantee that the blocks are going to pass. Many of the next blocks contain inaccurate data and do not guarantee the stability of the entire blockchain package.

On the other hand, with the help of computer processors, it may be possible to modify all the blocks at once. There is a solution called concrete proof that addresses this concern. This makes it possible for a customer to accelerate the pace of the construction of new buildings and apartments. It takes about 10 minutes to produce proof of work that is needed to mine new coins in the BTC blockchain. Miners perform this role of computation. Miners get to retain transaction fees as a bonus of mining [16, 17].

A copy of the entire blockchain network is received by each new user (node) joining the Ethereum network. This dataset has been sent to increase node inside the blockchain system after each block is created. Then, each node tests the information and finds that it is valid. If all goes well, each block is connected to the local blockchain.

A unanimous choice is reached by all the nodes in the blockchain system. When using the blockchain system, participation at all levels of the system is guaranteed due to the fact that people willingly abide by its laws.

Blockchain could solve the data protection issues on AI networks in modern computing world (e.g., IoT). AI and its implementations have become significant instruments for monitoring and processing [18, 19].

In order to ensure sufficient analytics in resolving security issues, the gathered data must be accounted for. Artificial intelligence (AI) is efficient and can be used in distributed computing if data entered into it is not manipulated or truthful.

Third-party blockchain, with contradicting input, can be used in different areas of cyberspace. Therefore, blockchain may have a great impact to decentralized systems.

Ensure authenticity, accuracy, and credibility of details. If information has credibility and is accurate, AI can do better. The possible course of study for this is to study the blockchain.

Businesses should ensure data security under B2B and M2M style setting.

5.5 *Blockchain Development of Networks*

When an individual, or a few, decide to embrace a blockchain technology, a network is built. This can be perceived as high-tech culture within these enterprises.

To give a clearer picture, let's use diamonds as an example. There are risks and difficulties involved with processing and selling the diamonds. Consumers would like to be sure they are acquiring diamonds from reputable and responsible businesses. Government agencies need the taxes to be collected and controlled. That framework of the blockchain will eradicate these potential risks.

In this network, the parties concerned include:

(a) Diamond manufacturers
(b) Institutions of the government
(c) Transporters with gems
(d) The sellers of diamonds

The same entities are assembled by blockchain solutions into a peer-to-peer network, which help to remove all the risks that had been listed and help to create a transparent system. All will be able to obtain the decentralized data of an immutable ledger and to track the flow of diamond from production to the final customer. In the public blockchain, all operations such as diamond mining, refining, and delivery are organized in sequence.

Under these blockchain networks, everybody has a complete copy (called peers). Also, there is ordering service to outline stuff that happened at the same time. Both those involved in the process have an oversight of the transactions (Fig. 4). There is

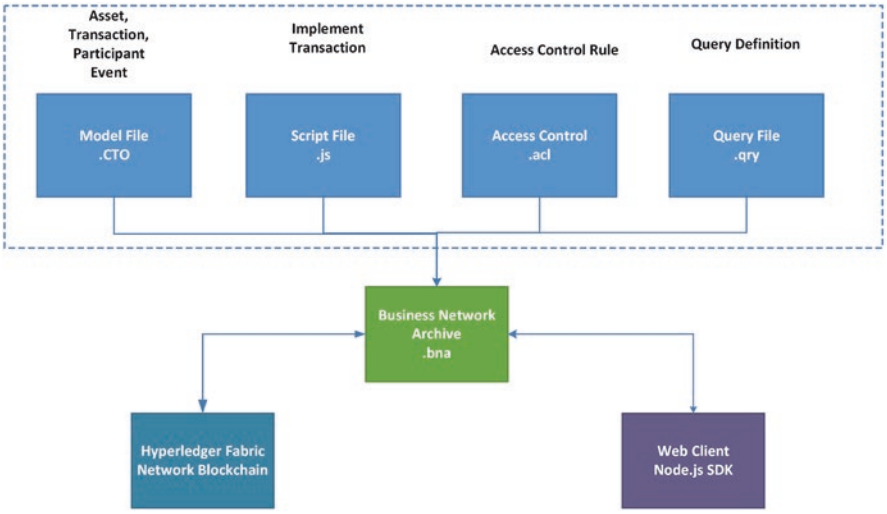


Fig. 4 Hyperledger composer

a member management system (MMS) for multiple users, which allows access to unique users within the network.

All transactions go through the general ledger during this phase (e.g., data with diamond photos, place of extraction, color, serial number, place where it was cut, purified, sold, etc.). This knowledge is reliable and true [20].

5.6 Key Characteristics of Blockchain Architecture

The blockchain architecture has many benefits for businesses. There are some attributes here.

Blockchain transactions are encrypted and checked because of their complex mathematical computations.

Immutability is permanent because records made cannot be altered or erased.

Provenance means that transactions can be trusted because they can be monitored online for a long time.

The entire various places are accessible by each member of the decentralized system. The consensus algorithm promotes network security.

Each user in the blockchain system is a generated address, not really a user identity. This will protect the privacy of users in a shared blockchain system.

Transparency cannot be manipulated by human. It is unlikely to happen because it takes too much computing power to rewrite the entire blockchain network.

Depending on how it is accessed and how the access permissions are issued, blockchain can be categorized into public, permissioned, and consortium blockchain [21, 22] (Fig. 5).

5.7 Key Features of a Blockchain Network

5.7.1 Public Blockchain

A public blockchain is a blockchain that anyone can access (often, anonymously). There are no limits on who can enter and, whether the transactions are mathematically legitimate, what transaction they can publish. Even though participants can secretly join the network (revealing only).

Any transaction they make is accessible to all (the public), which can be carefully analyzed in order to identify the users. The most popular example of decentralized blockchains is Bitcoin [3].

In such a network, there is usually an opportunity for participants to adopt an intensive consensus protocol for a computing resource (e.g., validate a block using proof of work).

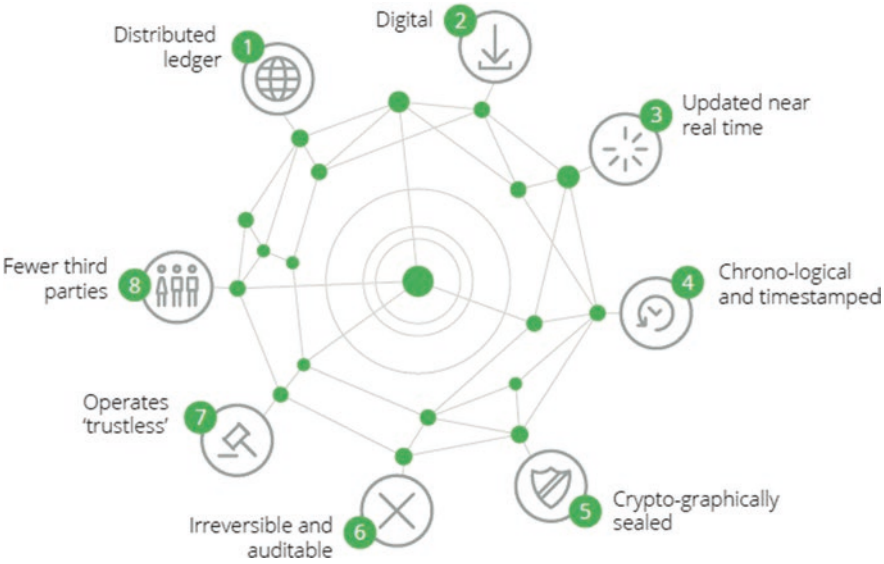


Fig. 5 Distributed domain feature of blockchain

5.7.2 Permissioned Blockchain

A permissioned blockchain is one in which the company's contact is limited to users who have access rights given by the owner of the network. Non-anonymous validation of blocks or contact with the blockchain is not allowed on such a network. To control access to such a network, a certificate authority (CA) is usually used. A platform running its network as an approved network by blockchain would decide who can be validators and what rights are provided to the users. One of the most famous examples of a permissioned blockchain system is Hyperledger Fabric [23–[25].

5.7.3 Consortium Blockchain

It is conceivable that the consortium blockchain (centralized) will be maintained by a single (originating) entity and offers predefined access rights to interacting parties. Usually, such a network suits government or regulatory bodies that have legal competence over other members.

In several cases, machine learning systems are used and have received great success, as shown below.

These types of patterns can be discovered by reviewing vast databases, such as stored medical records or credit history information. Machine learning techniques are used in places where we cannot get good results with conventional (deterministic) algorithms.

Several subjects require adaptable growth, for example, controlling manufacturing processes as per customer demand and adapting to readers' varied reading interests:

(i) In numerical data, supervised algorithms use statistical models in order to correctly identify the result. Regression and decision trees are the most commonly used algorithms in artificial intelligence.
(ii) ML does not contain label data. Here, the data points are grouped according to their statistical proximity or distance. K stands for algorithms for clustering and association rules. Supervised ML is a form of semi-supervised learning.
(iii) This project requires integrating both supervised and unsupervised machine learning. Unsupervised learning is implemented after which the most likely decisions are expected. It affects the data that lead [26–[28].

The model is then used as training data when constructing a new model.

Considering that more than half of the recorded cybersecurity blockchain applications were dealing with IoT devices, opportunities to optimize IoT security are obvious. There is a connection between IoT, military, and healthcare in Singapore (Fig. 6). The announcements of security breaches and attacks on IoT will create the market for approaches to IoT security threats.

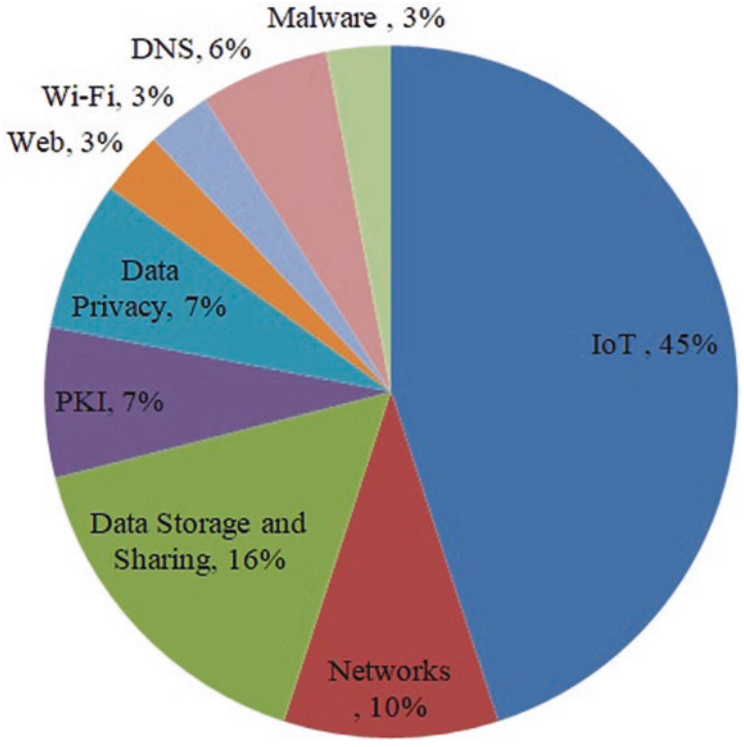


Fig. 6 Chart of themes of primary studies

Blockchain could solve the data protection issues on AI networks in modern computing world (e.g., IoT). Artificial intelligence (AI) and its applications are used in order to apply the security technique. The problem with big data is that if an AI's data is manipulated or misused by malicious third party, misleading analysis is the outcome. Blockchain can be used in different areas of cyberspace. Thanks to its decentralized and immutable features, blockchain guarantees data consistency, reliability, and honesty as well as reduces possibility of financial exploitation. If information has credibility and is accurate, AI can do better. Some blockchain research could include the implementation of AI data security in B2B (business-to-business) and M2M (machine-to-machine) environments [29, 30].

There are also questions about the validation and tamper resistance of main chains. We expect a distributed multi-blockchain infrastructure in the foreseeable future (Fig. 7).

This research sheds light on possibilities for research in cybersecurity other than IoT to be conducted. With the rising amount of users in the network using HTTPS encryption, cryptography needs to be safe and sound to ensure continued secure communications. Prospective research goal 1 in blockchain applications is to investigate the "Internet of Things" protection using Blockchain. Such data is unknown and hard to calculate for the purpose of this article. Future studies will include an in-depth evaluation of wireless network security, power consumption, and latency [31–[34].

IoT (Internet of Things) networks and data packets would need to be monitored and handled in order to enhance processes.

You can seek ways to overcome by exploring ideas and solutions using Ethereum and smart contracts. Researchers will want to explore how disruptive cybertechnology can be used in combination with blockchains.

Conclusion leads that, in the future, researchers could concentrate on developing decentralized applications and frameworks to protect the blockchain. However, decentralized cryptocurrencies such as Bitcoin have longer and more reliable

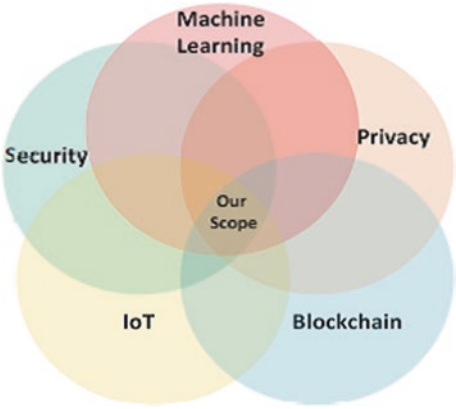


Fig. 7 Distribution status for the latest technology

blockchain (than decentralized cryptocurrencies such as Bitcoin) (e.g., ransomware and terrorism financing).

It is noted that permissionless blockchain systems typically take minutes to reach consensus, such as Bitcoin and Ethereum. For applications that are latency-sensitive including the Internet of Battlefield Things (IoBT), latency sensitivity may not be sufficient. Therefore, in combination with hardware-based approaches that have minimum latency, a future development objective is to design blockchain-based solutions [35].

Data has a significant role in training an ML model. We can use historical data of patients to predict how someone will respond with any new disease or medication. However, patients are hesitant to reveal their test results because of privacy concerns. Researches have worked to fix these issues. The researchers have developed a service called eDiag in order to collect user information and store them in a safe and supervised process. The previous study used quantitative reasoning methods that were not appropriate for online diagnosis. It was discovered that they achieved 94% accuracy without compromising data privacy. Likewise, the study examined the privacy issues as a question of learning privacy and model privacy, respectively (Tables 1 and 2).

Table 2 Objectives of the survey on data privacy

Objectives of survey	Merits	Demerits
To present the use of blockchain in intrusion detection	Scope of application of blockchain was discussed	Discusses only data sharing and trust management issues of collaborative intrusion detection
To discuss various security and privacy issues in Bitcoin	A comprehensive review of possible attacks on Bitcoin and provided countermeasures	Blockchain issues are not high-lighted
Survey on ML security solutions for Bitcoin	In-depth and wide classification of major threats and extensive explanation of the role of ML	Other applications of blockchain are missing
To study ML techniques for malware analysis	Time and space complexity for various methodologies has been described in detail	Lacks discussion on the uses of these techniques in a blockchain environment
Discuss applications, platforms, and protocols in blockchain specifically for AI	The decentralization feature of blockchain is explained with a specific view of AI	Discussion on privacy is not covered in detail
Review blockchain-based applications and identify open issues	Prerequisites for blockchain applications are thoroughly discussed	Focused on applications, not the open issues
To survey how ML can be used in blockchain-based smart applications	Discusses architecture and technology at a fundamental level and bridges the gap between the two technologies	–

6 Existing Solutions Using Blockchain Technology

The blockchain (BC) is a stable, fault-tolerant, open, verifiable, and auditable mesh network. Decentralized, P2P, open, confidence, and eternal are the commonly used keywords to explain BC benefits. These characteristics make a BC more trustworthy than an untrusted one.

Model for central client-server. The smart contract is a BC programming protocol that ensures that a scheduled operation is carried out. The blockchain, therefore, guarantees data integrity and authenticity, making it an effective solution for the protection of IoT devices against information theft.

Efforts to provide protection. Several supply chain, access control, application security, and IoT BC-based solutions have been suggested. However, the latest solutions do not comply with the time delay either, and cannot be extended to resource-restricted IoT devices [36, 37].

Some research, for example, focused only on the improvement of an IoT device's time response rather than its confidentiality and support. By breaking their BC architecture into three levels, i.e., IoT, fog, and cloud, they provided data integrity for cyber-physical systems (CPS) [38].

Using the Trustful Space-Time Protocol (TSTP), which is centered on confirmation, the IoT devices in the very same environment regain relationships with each other (PoT). Proof of luck (PoL) was used during the fog level to create responsibility to fix IoT information that generates a cryptographic digest for a data audit. SHA-256 was used to hash the data generated from the first level and saved temporarily. The data was permanently stored at the third level of the cloud, which is a public ledger, after acknowledgment and agreement had been achieved. Other than data integrity, key management utilizing time synchronization and node position was also provided by the report. HECOPS was used via multilateration to estimate the node's position, and clock synchronization was provided by TSTP. The paper suggested the use of several consensus points, such as PoT and PoL, but did not discuss any question of user privacy. The idea of securing data obtained from the drone using public BC was provided in another paper that provided data integrity. There were four modules presented by DroneChain; drones, management system, cloud server, and BC network. The control system managed the drone, and the software was encrypted and processed on a decentralized BC using a cloud server. The resulting system was trustworthy or accountable, provided immediate integrity of information, and had a resilient infrastructure. The study used PoW, however, which was not the best alternative for a real-time IoT application such as drones. In comparison, data provenance nor user/data protection was not provided by the network [39–41].

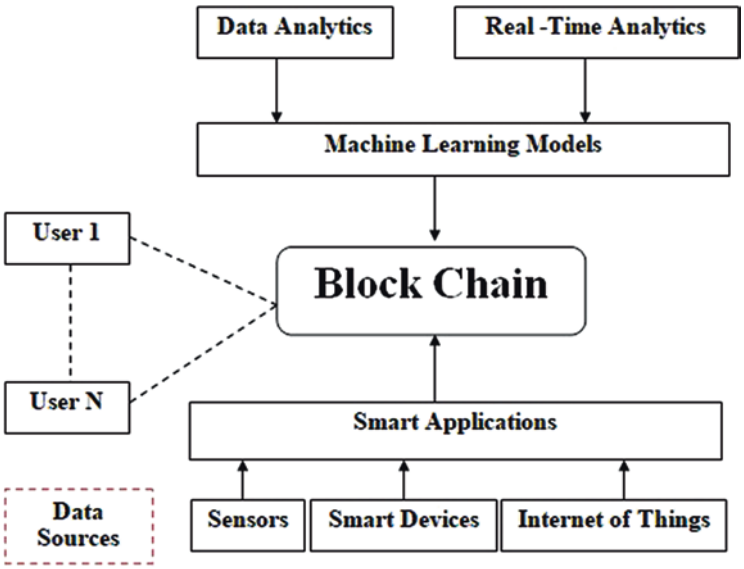


Fig. 8 Architectural diagram for data source with AI model

7 DeepChain Suggested a Value-Driven Reward System Based on BC to Solve Security Problems

For the model training process, DeepChain ensures data protection and auditability. Using the threshold Paillier method that offers an additive homomorphic property, confidentiality is used. Utilizing CNN algorithms and the MNIST dataset, DeepChain showed that even more parties were interested in the process.

The lower the preparation accuracy, the more collaborative training. To practice, ML classifiers require databases. Due to many privacy issues, such as data leakage, data integrity, and possession, these datasets are obtained from various entities that are typically unwilling to share their data. Users do not know how and when it is possible to use their knowledge [42] (Fig. 8).

8 Challenges to ML and BC

We assume that in providing maximum security and privacy for IoT networks, a single technology or tool, such as BC or ML, will not suffice. The research group is therefore in desperate need of time to investigate the provision of IoT security and privacy with the merger of BC and ML, which has the following challenges:

Storage: ML algorithms work better with bigger datasets, as described in Sect. 4. The growth of data on BC platforms, however, will degrade its performance.

To find a compromise, which would be perfect for IoT applications, open a research issue.

Latency challenges: An IoT network will produce a large amount of latency, depending on the scenario.

The volumes of information are more beneficial for deep learning. The overall speed of the ML system will accelerate. Both ML and BC have difficulty in terms of usability since both are computationally intensive.

Costs of response. Many machine learning algorithms use more power. It is normal in major IoT networks to anticipate increasing costs for wire access, routers, and switches. Similarly, when more users enter in a device, efficiency slows. On average, in the Ethereum, BC transactions are conducted at a rate too slow for a cryptocurrency. IoT software is where billions of transactions occur every second.

Vulnerability: The combination of ML and BC will dramatically increase security. There are some legal dilemmas as well.

The rise in the number of threats, particularly. Malicious and potentially malicious code increases in complexity with every passing day.

Real-time IoT networks. While it is possible, the training stage of ML would take a long time. This form of defense is only feasible when an eligible safety is on offer.

Blockchain technology. Information immutability can also be assured, and its adjustments can be specified. Moreover, there is considerable issue with the data on the blockchain. Besides that, it is not difficult to confirm whether equipment or sensors are malfunctioning prior to the problem. The device has been tried. Besides the above issues, BC is vulnerable to the risk of privacy disclosure. Methods are applied online and are available for all readers without cost [43].

Using third-person pronouns. As the data shows, there are also several opportunities raised in BC. The quantity of storage required for ML is extremely high. This move theoretically improves the average output (latency) of conventional models [44, 45].

Processing speed: It is difficult to identify vast volumes of data, because ML and BC are comparatively more data-consuming.

Communication costs. Many ML algorithms need extra processing and communication with increasing quantity of data transmitted that will lead to an increase of money expenses.

Often, the BC. As the number of users and nodes increase, congestion becomes more serious. On average, 90%, an Ethereum BC handles just 12 transactions per second, which is not possible in a conventional payment system.

Networks, where millions of transactions are taking place every second of the day. The combination of MBD and BB may have a major impact on economic and financial decisions. There are a few issues surrounding privacy in the present period. There is a rise in frightening circumstances. Malicious software and malware problem is difficult to identify and avoid. These are very useful in real-time IoT networks [46, 47].Although it is possible for most to go through the preparation, it could take a long time. Detection of malicious traffic is only possible with qualified models on the blockchain technology. It is possible to guarantee data immutability and to be able to define its transformations. However, because of the incorrect data,

this problem is occurring. Moreover, these early defects cannot be expected before anything happens suddenly.

The tests were completed and still have several things that are vulnerable to privacy evasion. The data is freely accessible for anyone to read it and analyze.

Getting private. BC is a solution to these problems but still restricted access in a way. There are abundant data available for ML to carry out its work [48, 49].

9 Conclusion

Blockchain and ML's recent developments have made them route developments. With the foundation of numerous intelligent applications such as smart cities, UAV, SG, and data trading, the distributed ledger has the potential to operate. We have provided extensive details on BT and ML in this paper, along with their uses in smart applications, and proposed an architecture based on ML-BT. An ML-BT-based data analysis framework can be developed and implemented using this architecture. It provides a discussion and comparison of various current surveys. Then, we implemented the taxonomy of the ML-BT solution, concentrating on objective-oriented, layer-oriented, countermeasures, and smart application dimensions. In each dimension, a comparative study of available methodologies and methods is presented. Then, during ML adoption in BT-based systems, we have listed several research challenges faced that require solutions. We also stressed a range of research opportunities that could serve as a future, such as the availability of infrastructure, quantum resilience, and privacy concerns.

References

1. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 29 June 2017)
2. N. Bozic, P. Guy, S. Stefano, A tutorial on blockchain and applications to secure network control-planes. SCNS IEEE 2016. [CrossRef]
3. D. Bradbury, The problem with bitcoin. Comput Fraud Secur. **11**, 5–8 (2013) [CrossRef]
4. G. Paul, P. Sarkar, S. Mukherjee, Towards a more democratic mining in bitcoins. In *Proceedings of the International Conference on Information Systems Security*, Hyderabad, India, 16–20 December 2014; Springer International Publishing: Cham, Switzerland, 2014
5. T. Bamert, C. Decker, R. Wattenhofer, S. Welten, BlueWallet: the secure BitcoinWallet, in *Security and Trust Management*, ed. by S. Mauw, C. Jensen, (Springer International Publishing, Cham, Switzerland, 2014), pp. 65–80
6. E. Anceaume, T. Lajoie-Mazenc, R. Ludinard, B. Sericola. Safety analysis of Bitcoin improvement proposals. In *Proceedings of the 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, 31 October–2 November 2016
7. R. Upadhyaya, A. Jain, Cyber ethics and cybercrime: a deep dwelved study into legality, ransomware, underground web and bitcoin wallet. In *Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA)*, Noida, India, 29–30 April 2016

8. S. Haber, W.S. Stornetta, How to time-stamp a digital document. In *Proceedings of the Conference on the Theory and Application of Cryptography*, Sydney, NSW, Australia, 8–11 January 1990; Springer: Berlin/Heidelberg, Germany, 1990
9. I. Eyal, G.S. Emin, Majority is not enough: Bitcoin mining is vulnerable. In *Proceedings of the International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014
10. K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, Systematic Mapping Studies in Software Engineering. In *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE)*, Bari, Italy, 26–27 June 2008
11. C. Mann, D. Loebenberger, Two-factor authentication for the Bitcoin protocol. In *International Workshop on Security and Trust Management*; Springer International Publishing: Cham, Switzerland, 2015
12. Y. Yuan, F.-Y. Wang, Towards blockchain-based intelligent transportation systems. In *Proceedings of the 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, Rio de Janeiro, Brazil, 1–4 November 2016
13. E.K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, B. Ford, École Polytechnique Fédérale de Lausanne (EPFL). Enhancing bitcoin security and performance with strong consistency via collective signing. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, USA, 10–12 August 2016
14. M. Vasek, M. Thornton, T. Moore, Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In *Proceedings of the International Conference on Financial Cryptography and Data Security*, Christ Church, Barbados, 3–7 March 2014; Springer: Berlin/Heidelberg, Germany, 2014
15. M. Bastiaan, Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin. Available online. http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-astochastic-analysis-of-two-phase-proof-of-work-in-bitcoin.pdf (accessed on 29 June 2017
16. M.H.U. Rehman, E. Ahmed, I. Yaqoob, I.A.T. Hashem, M. Imran, S. Ahmad, Big data analytics in industrial IoT using a concentric computing model. IEEE Commun. Mag. **56**(2), 37–43 (2018)
17. P.K. Sharma, J.H. Ryu, K.Y. Park, J.H. Park, J.H. Park, Li-Fi based on security cloud framework for future IT environment. HCIS **8**(1), 1–13 (2018)
18. W. Yu, F. Liang, X. He, W.G. Hatcher, C. Lu, J. Lin, X. Yang, A survey on the edge computing for the internet of things. IEEE Access **6**, 6900–6919 (2018)
19. M. Chiang, S. Ha, C.-L.I.F. Risso, T. Zhang, Clarifying fog computing and networking: 10 questions and answers. IEEE Commun. Mag. **55**(4), 18–20 (2017)
20. O. Novo, Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018)
21. K. Kalkan, S. Zeadally, Securing internet of things with software defined networking. IEEE Commun. Mag. **56**(9), 186–192 (2018)
22. B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
23. I. Butun, B. Kantarci, M. Erol-Kantarci, Anomaly detection and privacy preservation in cloud-centric internet of things. In *Proc. IEEE International Conference on Communication Workshop (ICCW)*, Jun 2015, pp. 2610-2615
24. S.R. Kumar, N. Gayathri, Trust based data transmission mechanism in manet using solsr. In *Annual Convention of the Computer Society of India* (pp. 169–180). Springer, Singapore., S. R., & Gayathri, N. (2016, December). Trust based data transmission mechanism in MANET using sOLSR. In *Annual Convention of the Computer Society of India* (pp. 169–180). Springer, Singapore
25. S.R. Kumar, N. Gayathri, B. Balusamy, Enhancing network lifetime through power-aware routing in MANET. Int. J. Internet Technol. Secur. Trans. **9**(1–2), 96–111 (2019)

26. HIMSS Blockchain Work Group. (2017, Oct. 23). Part 1: Navigating the blockchain landscape—Opportunities in digital health. [Online]. Available: http://www.himss.org/news/part-1-navigatingblockchain-landscape-opportunities-digital-health
27. D. Houlding, H. Flannery. (2018, Feb. 1). Part 2: Healthcare blockchain—A path to success in 2018. [Online]. Available: http://www.himss.org/news/part-2-healthcare-blockchain-path-success-2018
28. R. Rahim, R. Patan, R. Manikandan, S.R. Kumar, Introduction to blockchain and big data, in *Blockchain, Big Data and Machine Learning*, (CRC Press, 2020), pp. 1–23
29. HIMSS 2018 conference session. (2018, Mar. 6). Blockchain reset: Seeing through the hype and starting down the path. [Online]. Available: http://www.himssconference.org/session/blockchainreset-seeing-through-hype-and-starting-down-path
30. R. Chandran, S.R. Kumar, N. Gayathri, Designing a locating scams for mobile transaction with the aid of operational activity analysis in cloud. Wirel. Pers. Commun., **117**, 1–14 (2020)
31. The Linux Foundation. (2017). About Hyperledger. [Online]. Available: https://www.hyperledger.org/about Ethereum Foundation. (2018). Ethereum: Blockchain app platform. [Online]. Available: https://www.ethereum.org/
32. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman. (2016, Aug. 22–24). MedRec: using blockchain for medical data access and permission management, presented at the Int. Conf. Open and Big Data, Vienna, Austria. [Online]. Available: http://ieeexplore.ieee.org/document/7573685/
33. A.K. Show, A. Kumar, A. Singhal, N. Gayathri, K. Vengatesan, Future blockchain technology for autonomous applications/autonomous vehicle, in *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles*, (IGI Global), United States of America pp. 165–177
34. N. Kumar, N. Gayathri, M. A. Rahman, B. Balamurugan (eds.), *Blockchain, Big Data and Machine Learning: Trends and Applications*, United States of America (CRC Press, 2020)
35. C. McFarlane, M. Beer, J. Brown, N. Prendergast. (2017, May). Patientory: a healthcare peer-to-peer EMR storage network v1.1. [Online]. Available: https://patientory.com/patientory_whitepaper.pd.
36. S.K. Sharma, R.K. Modanval, N. Gayathri, S.R. Kumar, C. Ramesh, Impact of application of big data on cryptocurrency. Cryptocurrencies and Blockchain Technology Applications, Scrivener Publishing LLC, Beverly, Massachusetts. 181–195 (2020)
37. A. Pandey, A. Kumar, A. Singha, N. Gayathri, S.R. Kumar, 4 Blockchain Databases 2. *Blockchain, Big Data and Machine Learning: Trends and Applications*, 97 (2020)
38. R. Chandran, S.R. Kumar, N. Gayathri, Genetic algorithm-based tabu search for optimal energy-aware allocation of data center resources. Soft. Comput. **24**(21), 16705–16718 (2020). https://doi.org/10.1007/s00500-020-05240-9
39. L. Dong, W. Jinwu, Block chain technology principle, application field and challenge [J]. Telecomm. Sci. **32**(12), 19–25 (2016)
40. Y. Yong, W. Feiyue, Development status and Prospect of block chain technology [J]. Acta Automat. Sin. **42**(4), 481–494 (2016)
41. G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. & Applic. **32**(3), 639–647 (2020)
42. C. Gao, T. Liang, L.I. Huixing, et al., Development and Application of open automated demand response [J]. Power Syst. Technol. **93**(3), 12–12 (2013)
43. R.K. Sakthivel, G. Nagasubramanian, F. Al-Turjman, M. Sankayya, Core-level cybersecurity assurance using cloud-based adaptive machine learning techniques for manufacturing industry. Trans. Emerg. Telecommun. Technol., e3947 (2020)
44. W. Beibei, S. Yujun, L. Yang, Application of uncertain demand response modeling in power integral incentive decision [J]. Automat. Electr. Power Syst. 2015(10). R.M. Parizi, On the gamification of human-centric traceability tasks in software testing and coding. In: *2016 IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)*, Towson, MD, 2016, pp. 193–200

45. A. Back, et al., Enabling blockchain innovations with pegged sidechains [Online]. Available: http://www.blockstream.com/sidechains.pdf, 2014
46. P. Robinson, Requirements for Ethereum Private Sidechains, arXiv Prepr. arXiv1806.09834, 2018
47. Q. Zhang, R.M. Parizi, K.K.R. Choo, A pentagon of considerations towards more secure Blockchains. IEEE Blockchain Tech. Briefs. pp. 1–30 (2018)
48. Bitcoin-abe, https://github.com/bitcoin-abe/bitcoin-abe
49. T.T.A. Dinh, J. Wang, G. Chen, R. Liu, B.C. Ooi, K.-L. Tan, BLOCKBENCH: a framework for analyzing private blockchains. In: *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, p. 10851100

Correction to: Review of Cryptocurrencies Implementations in the Cloud Environment: Ethereum in the Cloud

Aicha Bouichou, Soufiane Mezroui, and Ahmed El Oualkadi

Correction to:
Chapter 5 in: K. M. Baalamurugan et al. (eds.), ***Blockchain Security in Cloud Computing*****, EAI/Springer Innovations in Communication and Computing,**
https://doi.org/10.1007/978-3-030-70501-5_5

This chapter was inadvertently published without updating the following error.

The name and affiliation information of the authors "Aicha Bouichou, Soufiane Mezroui and Ahmed El Oualkadi" was erroneously published in chapter 5. This has been updated in this corrected version.

The updated online version of this chapter can be found at
https://doi.org/10.1007/978-3-030-70501-5_5

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5_15

Index

K. M. Baalamurugan et al. (eds.), *Blockchain Security in Cloud Computing*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-70501-5