SPRINGER BRIEFS IN COMPUTER SCIENCE

Ahmed Imteaj
M. Hadi Amini
Panos M. Pardalos

Foundations of Blockchain

Theory and Applications

Springer

SpringerBriefs in Computer Science

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic.

Typical topics might include:

- A timely report of state-of-the art analytical techniques
- A bridge between new research results, as published in journal articles, and a contextual literature review
- A snapshot of a hot or emerging topic
- An in-depth case study or clinical example
- A presentation of core concepts that students must understand in order to make independent contributions

Briefs allow authors to present their ideas and readers to absorb them with minimal time investment. Briefs will be published as part of Springer's eBook collection, with millions of users worldwide. In addition, Briefs will be available for individual print and electronic purchase. Briefs are characterized by fast, global electronic dissemination, standard publishing contracts, easy-to-use manuscript preparation and formatting guidelines, and expedited production schedules. We aim for publication 8–12 weeks after acceptance. Both solicited and unsolicited manuscripts are considered for publication in this series.

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

More information about this series at http://www.springer.com/series/10028

Ahmed Imteaj • M. Hadi Amini
Panos M. Pardalos

Foundations of Blockchain

Theory and Applications

Springer

Ahmed Imteaj
Florida International University
Miami, FL, USA

M. Hadi Amini
Florida International University
Miami, FL, USA

Panos M. Pardalos
University of Florida
Gainesville, FL, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-030-75024-4 ISBN 978-3-030-75025-1 (eBook)
https://doi.org/10.1007/978-3-030-75025-1

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

Preface

This book provides a comprehensive analysis of fundamental topics related to blockchain. It explores different vital issues and specific application areas that can benefit from blockchain. The authors present the elementary description, visualize the working procedure of the blockchain paradigm, and highlight the areas it can be applied in real life. The main focus of this book is to explain blockchain and its application from a new perspective, that is, distributed Internet of Things (IoT) and interdependent networks.

Miami, FL, USA — Ahmed Imteaj

Miami, FL, USA — M. Hadi Amini

Gainesville, FL, USA — Panos M. Pardalos

Contents

About the Authors

Ahmed Imteaj is currently a PhD candidate and graduate assistant at the Knight Foundation School of Computing and Information Sciences, Florida International University, under the supervision of Professor M. Hadi Amini. He is also a research lab member of Sustainability, Optimization, and Learning for InterDependent networks laboratory (solid lab) at Florida International University. His research interests span federated learning, machine learning, internet of things (IoT), smart systems, and Blockchain. He holds a B.Sc. degree in Computer Science and Engineering from Chittagong University of Engineering and Technology (CUET), Bangladesh in 2015. From 2015 to 2018, he worked as a Lecturer at International Islamic University Chittagong (IIUC), Chittagong, Bangladesh. Ahmed's work on federated learning for IoT environments is the recipient of the best paper award from "2019 IEEE Conference on Computational Science & Computational Intelligence" and won the second place at 2021 Florida International University Graduate Student Appreciation Week. He has published more than 30 referred journals and conference papers.

M. Hadi Amini is an assistant professor in the Knight Foundation School of Computing and Information Sciences at Florida International University. He is the director of Sustainability, Optimization, and Learning for InterDependent networks laboratory (www.solidlab.network). He received both his Ph.D. in electrical and computer engineering in 2019 and M.Sc. degree in 2015 from Carnegie Mellon University. He also holds a doctoral degree in computer science and technology. Prior to that, he received an M.Sc. degree from Tarbiat Modares University in 2013 and a B.Sc. degree from Sharif University of Technology in 2011. His research interests include distributed optimization and learning algorithms, distributed computing and intelligence, sensor networks, interdependent networks, and cyber-physical-social resilience. Application domains include smart cities, energy systems, transportation electrification, and healthcare.

Hadi is a life member of IEEE-Eta Kappa Nu (IEEE-HKN), the honor society of IEEE. He served as the president of Carnegie Mellon University Energy Science and Innovation Club, as technical program committee of several IEEE and ACM conferences, and as the lead editor for a book series on sustainable interdependent networks since 2017. He also serves as associate editor of SN Operations Research Forum and International Transactions on Electrical Energy Systems. He has published in more than 100 refereed journals and conference papers and book chapters. He edited/authored six books. He is the recipient of the best paper award at the 2019 IEEE Conference on Computational Science & Computational Intelligence, 2020 Excellence in Teaching Award from the School of Computing and Information Sciences at Florida International University, best reviewer award from four IEEE Transactions, the best journal paper award by the Journal of Modern Power Systems and Clean Energy, and the dean's honorary award from the president of Sharif University of Technology. (Homepage: www.hadiamini.com)

Panos M. Pardalos is a distinguished professor and the Paul and Heidi Brown preeminent professor in the Departments of Industrial and Systems Engineering at the University of Florida, and a world-renowned leader in global optimization, mathematical modeling, and data sciences. He is a fellow of AAAS, AIMBE, and INFORMS and was awarded the 2013 Constantin Caratheodory Prize by the International Society of Global Optimization. In addition, Dr. Pardalos has been awarded the 2013 EURO Gold Medal prize bestowed by the Association for European Operational Research Societies. This medal is the preeminent European award given to operations research (OR) professionals for "scientific contributions that stand the test of time." Dr. Pardalos is also a member of the New York Academy of Sciences, the Lithuanian Academy of Sciences, the Royal Academy of Spain, and the National Academy of Sciences of Ukraine. He is the founding editor of Optimization Letters, Energy Systems, and co-founder of the International Journal of Global Optimization. He has published over 600 papers, edited/authored over 200 books, and organized over 80 conferences. He has about 57,000 citations on his work, an H-index of 95, an $i10$- index of 575 (Google Scholar), and has graduated 62 Ph.D. students so far.

Part I
Blockchain Theory

Chapter 1
Introduction to Blockchain Technology

This chapter introduces blockchain's fundamental topics, including the definition, components, how blockchain works, key characteristics, taxonomy, applications, advantages, and limitations (Fig. 1.1).

1.1 What Is Blockchain Technology?

A *blockchain* is a distributed and decentralized ledger consisting of blocks that hold transaction records or history. The ledger is distributed among all the network agents, and no central entity (i.e., decentralized) controls the overall processing of the system [1]. The nodes or agents that are involved within a blockchain network are called participants and miners. The participants are simply the agents who perform any transaction, and the miners are responsible for validating or rejecting a block. Inside a block, there may be contract records of anonymous parties, payment or reward histories, data ownership information, etc. Each block has a fixed capacity, and when there is no more space within a block, further data are added to a new block. However, if new blocks are added at a high rate, then it causes performance problems. The authors in [2] proposed "Inclusive Block Chain Protocols" that accelerate transaction speed, and further investigation is required to verify whether the new technology can overcome the performance problems (Table 1.1).

A blockchain is also called a *Chain of Blocks* as each block is linked with its previous block by keeping the previous block's hash information. The hash is generated based on the block information, and any changes within the block generate a different hash. Therefore, even any slight changes within a block result in breaking the whole chain as the subsequent block cannot locate the tampered block due to hash mismatch. The largest chain is selected as the best chain in such a situation, and eventually, tampered blockchain is omitted.

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_1

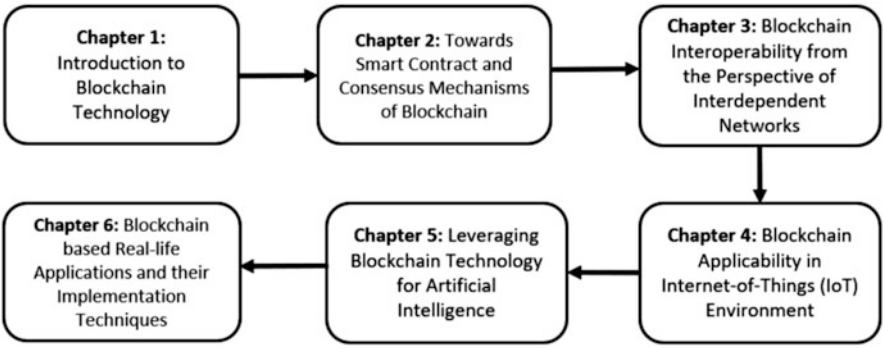

Fig. 1.1 An overview of book chapters

Table 1.1 Blockchain terminology

Term	Meaning
Blockchain	The main authentic ledger
Blockchain technology	The technology involved in simulating the overall architecture of the blockchain
Blockchain network	A network in which the blockchain exists
Blockchain generation	A particular blockchain
Blockchain user	A person, institution, organization, business, department, or government who is a part of the blockchain network

1.2 Blockchain Components

Blockchain technology consists of several components, including some cryptographic mechanisms (e.g., cryptographic hash function, cryptographic nonce) and data storage concept (e.g., ledger). To simplify the basic understanding, this section covers the details of the main components of blockchain: cryptographic hash function, cryptographic nonce, transactions, asymmetric-key cryptography, address and address derivation, blocks, and chaining of blocks.

1.2.1 Cryptographic Hash Functions

The operation of blockchain technology is remarkably dependent on the concept of the cryptographic hash function. Hashing is simply a technique of applying

cryptographic hash function to existing data that calculates a unique output (called *digest*) for a given input data.

It allows individuals to independently take input data, hash that data, and derive the same result, proving no change in the data. Even the smallest change to the input (e.g., changing a single bit) will result in a completely different output digest. Table 1.2 shows simple examples of this.

1.2.2 Transactions

The interaction between parties is represented as a transaction. A transfer of cryptocurrency between the users can be regarded as a transaction for the blockchain network users [3]. The valid transactions are stored within a block, and each block may hold zero or more transactions. Typically in a blockchain environment, constant creation of new blocks, even with no transaction, is crucial for maintaining security as it prevents malevolent users from creating a longer, tampered blockchain. While making a transaction, a blockchain network user sends information that includes the sender's address and public key, asymmetric cryptography-based digital signature (details in Sect. 1.2.3), transaction inputs, and outputs. The transaction inputs that resemble the list or quantity of digital assets need to be transferred, while the transaction outputs indicate how much assets the receiver is supposed to receive.

1.2.3 Asymmetric-Key Cryptography

In a blockchain network, asymmetric-key cryptography establishes a trust relation between blockchain users to verify authenticity, non-repudiation, confidentiality, and integrity of transactions while keeping those transactions public [4]. Each blockchain user owns a public key and a private key. The private key is used for signing or encrypting a transaction, which is spread over the blockchain network, while the public keys are visible to all users of the blockchain network, and they can be used to decrypt the transaction. In this way, it ensures authenticity, i.e., the receiver can understand that the authenticated user signs the transaction. However, this does not ensure confidentiality. The sender can encrypt the transaction with its

Table 1.2 Examples of some input data sample and corresponding SHA-256 generated values

Input data	SHA-256 hash value
Solid lab	bb909246de94465e22908c5f02714eaab2a596e9d8f965fa9b3566cecfef7881
Solid lab	ee918c14b5d41be9eb3906e4d6d456c33ce36fffa4729e3d4285db280d285a58
FIU	71f85e67a8f330bceb32057581b450710ce96fdcb1d04649e20256e7090298c9
FIU CS	7ded8a91d8d7d663cfca5fc5e22dd05c2c3f047d0d00c8bfedee7b952fd8d940

private key and the receiver's public key to achieve this. After that, the receiver can decrypt it using its own private key and the sender's public key.

1.2.4 Block

A blockchain block consists of a block header and block body. The block header holds the following properties:

- *Previous Block Hash*: A 256-bit hash value generated by the previous block. This hash value helps us to track the previous block and make a link.
- *Timestamp*: The current time of block creation.
- *Merkle Tree Root*: The block hash generated from the available transactions.
- *Nonce*: The full abbreviation of *nonce* is "number only used once." The blockchain miner needs to solve or discover a number before participating in the validation of a block. Upon solving or discovering the number, the miner is given cryptocurrency for their efforts. The nonce is a way to exclude the less potential crypto miners. The block data is combined with a nonce to produce a unique hash digest: *hash (data + nonce) = Unique digest value*

The block body consists of a transaction counter and a list of transactions. The number of the transactions a block can hold depends on the size of the block and also the size of the transactions. An asymmetric cryptography technique (i.e., digital signature) is used to validate the originality of the transactions (Fig. 1.2).

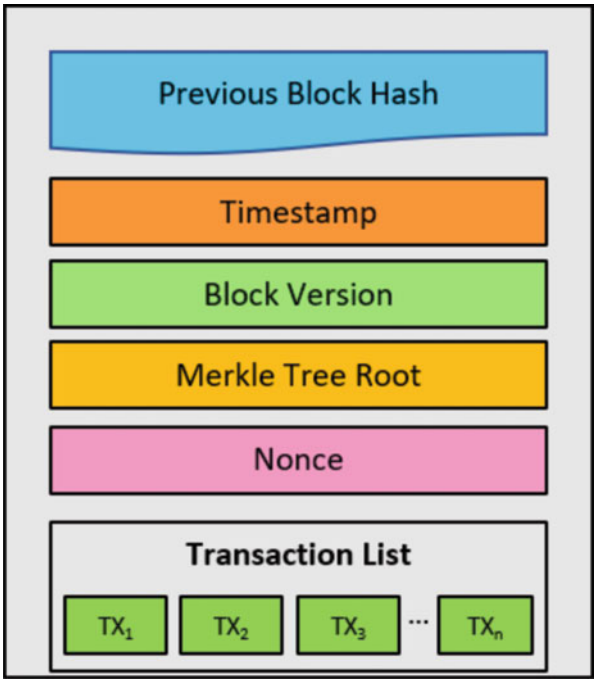

Fig. 1.2 A representation of a block structure

1.2.5 Chaining Blocks

In a blockchain, the blocks are linked together as each block holds the hash value of its previous block (parent block). Figure 1.3 represents a generic blockchain with a sequence of blocks. If the parent block is somehow altered, e.g., any transaction record is changed, then the hash value will be changed, as we discussed in Sect. 1.2.1 that a simple change within the data would generate a completely different hash. The modification of a single block will disconnect all subsequent blocks, as the child block holds the untampered block hash and will no longer be linked to the tampered block. Therefore, the chain will be broken. Meanwhile, if all the blocks have unaltered data, then the hash value will be the same, i.e., each block can track its parent block, and eventually, it produces a longer blockchain. Figure 1.4 represents how a tampered blockchain would hold fewer blocks and not be considered the main chain.

1.3 How Blockchain Works

When a user joins a blockchain network and requests for a transaction, it is broadcasted over the peer-to-peer (P2P) network. The users (nodes) within the network verify the transaction through a consensus mechanism [e.g., proof of work (PoW), proof of stake (PoS)]. The details of the consensus mechanism are discussed

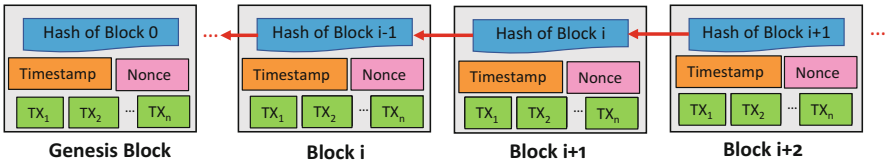

Fig. 1.3 A representation of a blockchain that consists of a sequence of blocks

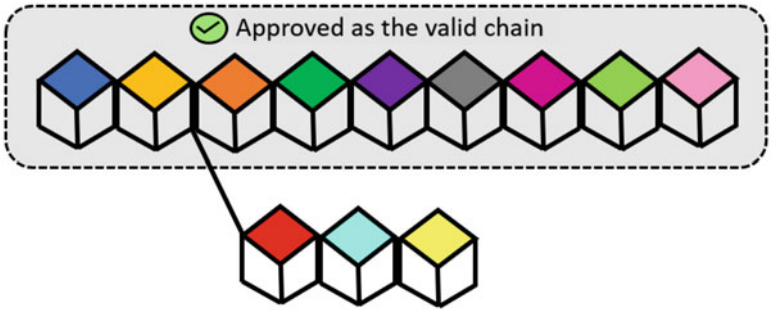

Fig. 1.4 Approval of the longer blockchain as the valid one

in the next chapter. After the transaction is verified, it is included within a block. After the inclusion of necessary transactions, block requests are to be included in the chain. Before including a block within the chain, the blockchain miner checks the block for validation to avoid any alteration or tamper of any data. If the block is validated, then it is appended to the main chain; otherwise, it is eliminated and not included in the main chain. After that, the transaction becomes complete, and there remains no possibility of changing the transaction history (Fig. 1.5).

1.4 Key Characteristics of Blockchain

In this segment, we point out the key characteristics of blockchain and describe how the features play a vital role in improving a system. The combination of all key features makes a blockchain superior to the conventional approach (Fig. 1.6).

1.4.1 Decentralization

In the conventional centralized approach, each transaction is validated through a central entity that encounters performance bottlenecks and extra costs. However, in a blockchain-based system, a transaction can be carried out through a peer-to-peer authentication scheme without any need for a central agency. Therefore, the

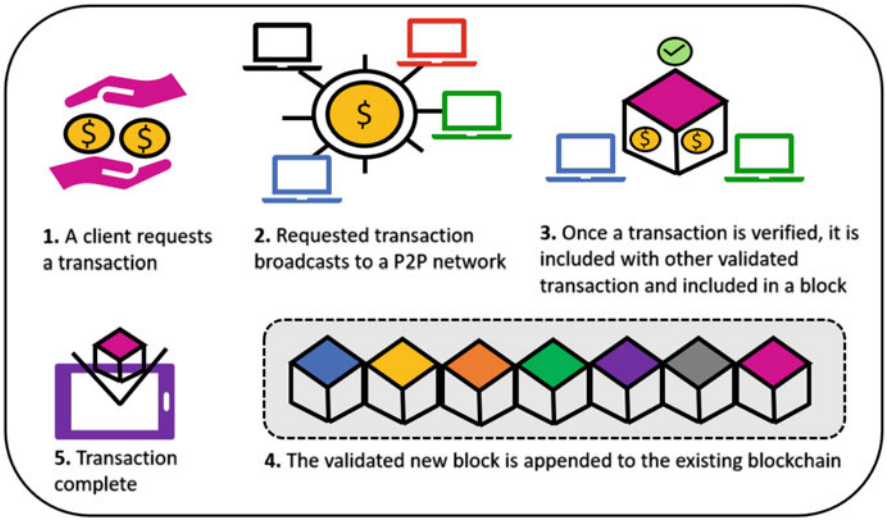

Fig. 1.5 The working mechanism of a blockchain

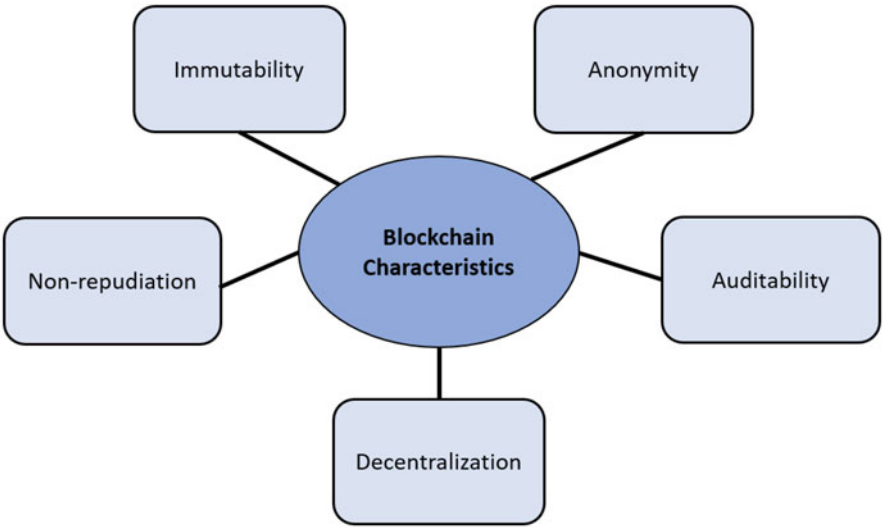

Fig. 1.6 Characteristics of blockchain

costs related to development, maintenance, and operational costs are significantly reduced, and the performance bottleneck of the server is mitigated.

1.4.2 Immutability

The valid transactions are included in the block, and the updated ledger is spread over the blockchain network. Any slight changes or tamper of any information is not feasible because any changes of data within a block change the hash values that eventually break the chain. Therefore, any tampered block cannot pass the validation stage, and any falsification would be easily detected.

1.4.3 Anonymity

In a blockchain network, there is no central agency to keep users' private information. That means none of the participants of the blockchain network need to share their identity with a third party. Instead, each user participates and interacts with other blockchain clients by generating one or more addresses. The addresses are used while establishing communication, making a transaction, or signing any contract. The private information of a user is not revealed to avoid identity disclosure, and such a strategy preserves privacy.

1.4.4 Auditability

As we mentioned in Sect. 1.2.4, each block has a field to store the block creation time, called timestamp. Each transaction within a block also holds a timestamp to indicate when the transaction is processed. Furthermore, any modification of the transaction or block information change can be easily traced by other nodes within the network. The other user can trace any previous record that is stored in any node of the distributed system by going back iteratively using the previous information hash. In this manner, the auditability characteristic improves blockchain transparency.

1.4.5 Non-repudiation

Non-repudiation is another key charismatic of blockchain. It means that none of the participants can deny the occurrence of a transaction event or its behavior. The primary purpose of non-repudiation is to collect and store, maintain, supply, and verify any undeniable evidence about messages between blockchain participants. The non-repudiation is applicable in two aspects: (1) a sender "Bob" sends a message to a receiver "Alice." "Bob" cannot decline the action. (2) Similarly, "Alice" cannot deny that he did not receive that message. Blockchain uses asymmetric encryption, e.g., digital signatures, to assure the non-repudiation feature.

1.5 Taxonomy of Blockchain

This section will classify and compare different blockchain structures that would be helpful while designing blockchain-based software architectures. We capture each blockchain's major characteristics, including the performance, consensus, and quality attributes from various prior works, e.g., [5–7].

1.5.1 Public Blockchain

In a public blockchain, anyone can join and see the transactions on the network. To participate in a public blockchain is a matter of downloading of required software. Public blockchain cuts down the need to keep an intermediary in controlling blockchain network or any asset exchanging scenario. That means a public blockchain works entirely in a decentralized way. All the operations or activities within a blockchain network are accomplished through peer-to-peer mechanisms. Every node within the network verifies every transaction before it is included in

the system. Any node can sync the entire blockchain and can observe the overall blockchain history. This feature makes public blockchain extremely secure while slowing down the overall process due to many nodes.

1.5.2 Private Blockchain

Private or permissioned blockchain considers a middleman responsible for selecting the nodes that can be part of the network. Besides, the central entity has the power of validation and can change any rule of the blockchain (e.g., block consensus). Only the selected nodes have access to view the blockchain ledger or make any contribution. Usually, private blockchains are smaller in size as a limited number of people are considered to join the system. Private blockchain is incredibly beneficial for small corporations, agencies, or organizations. Due to the full power central entity, a private blockchain is comparatively less secure but has faster operations than a private blockchain.

1.5.3 Consortium Blockchain

The consortium blockchain is a combination of both public and private blockchains. A notable difference can be noticed at the consensus level. Instead of considering an open platform where anyone can validate a block or a closed system where only a single authority has the validation power, a consortium blockchain considers equally powered entities as the validators. That means, if a certain fraction of these parties behave honestly, then the overall system will not face any trouble. A consortium blockchain is appropriate where multiple organizations work together in the same platform and look for a common ground to carry out transactions and any relay information.

Property	Public	Private	Consortium
Decentralized	Yes	No	Partially
Immutability	Very difficult to tamper	Alterable	Partially immutable
Non-repudiation	Not refusable	Easily refusable	Partially refusable
Consensus decision	All miners	A set of nodes	An organization
Consensus decision	Public, permissionless	Permissioned	Permissioned
Transparency	Completely transparent	Not transparent	Partially transparent
Efficiency	Low	Very high	High
Flexibility	Poor	Very good	Good

1.6 Examples of Blockchain Applications

In this section, we list some of the prominent sectors where blockchain technology can be deployed. Examples of some emerging blockchain application domains are listed below:

- Secure storage and exchanging of medical records
- Real-time traffic monitoring
- Energy market trading
- Stock market
- Voting mechanism
- Supply chain management
- Financial service
- Smart parking
- Street light management
- Waste management
- Insurance
- Farming
- Education.

The detailed discussion on blockchain applications is presented in Chap. 6.

1.7 Advantage and Limitations of Blockchain

There are a wide spectrum and numerous benefits of blockchain technology, including decentralization, anonymity, persistency, and auditability. On the other hand, blockchain technology has some limitations that need to be considered while designing a system. A comprehensive overview of blockchain opportunities and their limitations is presented in [8–10].

Pros

1. Transaction are secure and private.
2. The accuracy is improved due to inconsideration of human involvement or disregard of any paperwork.
3. All transactions are transparent.
4. Eliminate the need for third-party verification.
5. A decentralized ledger is stored in all available users which makes it difficult to tamper any content within the ledger.

Cons

1. If the consensus mechanism is not strong, then the transaction verification process would be biased.
2. The technology cost to conduct the overall process is high.

3. No types of blockchain ensure both strong security and faster process at the same time. For instance, public blockchain is more secure, but the verification process is slower. In contrast, private and consortium blockchains are faster but less secure due to issues of centralization.

1.8 Discussion

Blockchain is a distributed ledger that ensures immutability, authentication, confidentiality, and non-repudiation of a transaction and avoids any alteration or refusal of an established contract. The user information is replaced with an address that hides the personal identity. All the available network users verify a transaction, and only the validated blocks are approved for inclusion in the main chain. Only the untampered or original blocks are remained in the main chain, while the disapproved and altered blocks are excluded.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Manubot (2019)
2. Lewenberg, Y., Sompolinsky, Y., Zohar, A.: Inclusive block chain protocols. In: International Conference on Financial Cryptography and Data Security, pp. 528–547. Springer, Berlin, Heidelberg (2015)
3. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media (2015)
4. Yaga, D., Mell, P., Roby, N., Scarfone, K.: Blockchain technology overview. Preprint (2019). arXiv:1906.11078
5. Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., Rimba, P.: A taxonomy of blockchain-based systems for architecture design. In: 2017 IEEE International Conference on Software Architecture (ICSA), pp. 243–252. IEEE (2017)
6. Tasca, P., Tessone, C.J.: Taxonomy of blockchain technologies. Principles of identification and classification. Preprint (2017). arXiv:1708.04872
7. Labazova, O., Dehling, T., Sunyaev, A.: From hype to reality: A taxonomy of blockchain applications. In: Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019) (2019)
8. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., Wang, H.: Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
9. Hughes, L., Dwivedi, Y.K., Misra, S.K., Rana, N.P., Raghavan, V., Akella, V.: Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. Int. J. Inf. Manag. **49**, 114–129 (2019)
10. Ducrée, J.: Research–A blockchain of knowledge? Blockchain Res. Appl. **1**(1–2), 100005 (2020)

Chapter 2
Toward Smart Contract and Consensus Mechanisms of Blockchain

This chapter presents a detailed description of smart contract and proof-based consensus mechanisms used in blockchain technology. Smart contracts are used in blockchain technology while making transaction between two parties, and it enables only the validated transaction to be included in the blockchain. However, to validate a transaction, Satoshi Nakamoto, who is the inventor of blockchain, introduced a proof-of-work (PoW) consensus algorithm while performing transaction among blockchain nodes (i.e., users) [1]. Later on, various proof-based consensus mechanisms [e.g., proof of stake (PoS), proof of location (PoL), PBFT (practical Byzantine fault tolerance)] are proposed. The main concept of applying proof-based algorithms is that the nodes within the blockchain network that performs and exhibits sufficient proof will get the privilege to append a new block to the main chain and collect the reward. In this chapter, we present a clear explanation of smart contract and discuss about some of the most important consensus algorithms of blockchain that are widely used (Fig. 2.1).

2.1 Smart Contract

A smart contract is an important part that contributed to the advancement of blockchain technology (Fig. 2.2). Smart contracts were introduced in the 1990s as a computer-based transaction protocol that can document, control, and execute legal events and perform actions based on the contract agreement [2]. The main objectives of integrating smart contracts in blockchain technology are to reduce the need for trusted intermediators and fraud losses and to reduce the malicious, enforcement costs, and accidental exceptions [3]. A smart contract is implemented on top of the blockchain technology. In a smart contract, when two parties agreed on all the clauses stated in a smart contract and start the transaction, it is automatically embedded into the blockchain and proceeded when certain clauses or conditions are

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_2

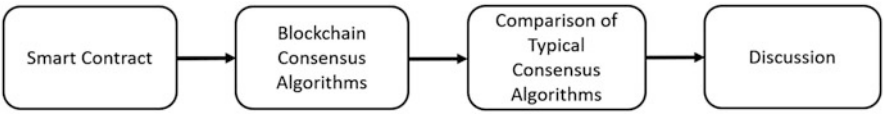

Fig. 2.1 Chapter overview

fulfilled (e.g., a party gets penalty or punishment when it breaches the smart contract clauses). The contractual clauses of a smart contract are transformed into executable computer programs. The logical connections that exist among the contractual clauses are preserved in the form of program logic flows (e.g., if-else-if statements) [4]. A contract statement that is executed cannot be further modified, i.e., the transaction is recorded as immutable in the blockchain. Besides, smart contracts facilitate access control of each smart contract function. That means it is possible to set access permission for different functions of smart contracts. Moreover, smart contracts ensure contract enforcement, i.e., it guarantees that the execution of smart contract is deterministic. In particular, whenever any smart contract conditions are satisfied, it automatically triggers the corresponding function. For instance, two users of a blockchain network named Alice and Bob give their consent on the penalty or punishment of violating a smart contract agreement. If Alice breaches the contract, then immediately, the penalty mentioned in the smart contract will be cut from Alice's deposit. The life cycle of a smart contract has four phases: creation, execution, deployment, and finalization or completion [4, 5], which is illustrated in Fig. 2.3.

2.1.1 Creation of a Smart Contract

At the beginning of a contract creation, the involved parties perform negotiation on the rights, obligations, and prohibitions on that contract. All the involved parties reach to an agreement after multiple rounds of negotiations and discussions. A draft of an initial contractual agreement is prepared by the lawyers or counselors of the involved parties. After that, the agreement written in natural languages is converted into a programmable language that may include declarative and logic-based rule language [5, 6]. The conversion of a smart contract from a natural language to a computer-based language is composed of several stages, i.e., contract design, deployment, testing, and validation, like software development. After several iterative processes, a smart contract is prepared and published in the blockchain.

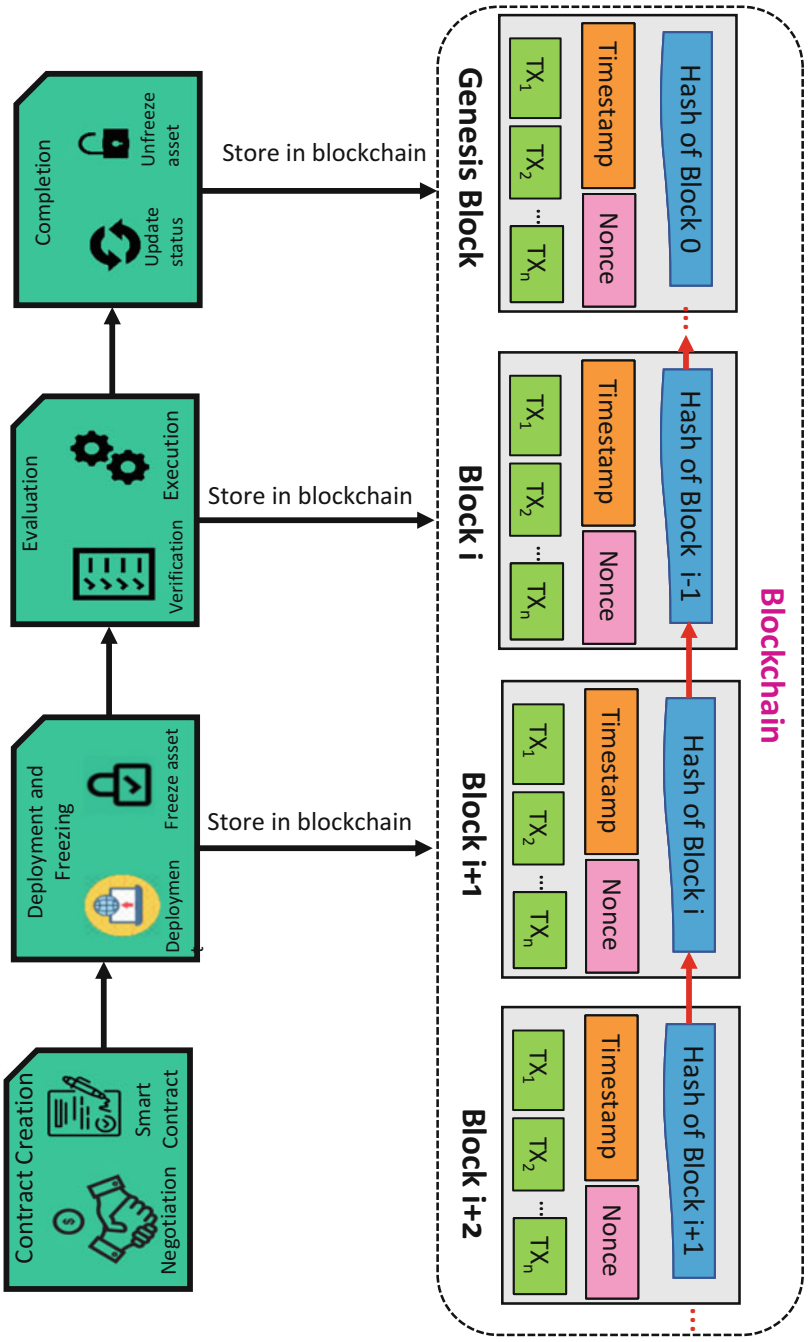

Fig. 2.2 Steps of preparing a smart contract

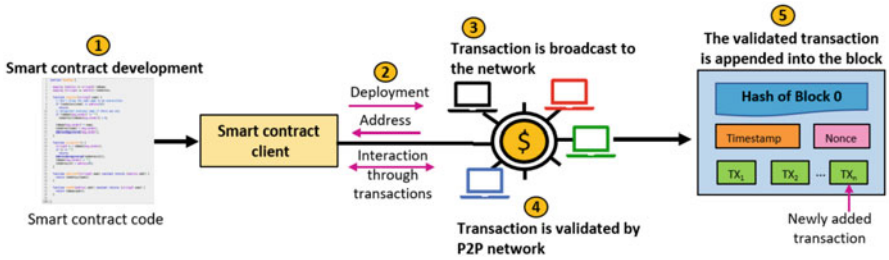

Fig. 2.3 Life cycle of a blockchain smart contract

2.1.2 Deployment of a Smart Contract

After the smart contract is prepared, it is validated and deployed on top of a blockchain. After a contract is published on a blockchain, it cannot be modified due to blockchain immutability. Any correction or modification requires creating a new contract. When a contract is published and implemented on the blockchain, it is accessible to all the available parties. In the meantime, the involved parties' digital assets are frozen via their digital wallets, and those digital wallets are sued to identify the parties [7].

2.1.3 Execution of a Smart Contract

After the smart contract is deployed in blockchain, the contractual clauses are monitored and evaluated. Whenever a contractual condition meets (e.g., receive the contractual product), the sequential related procedures are automatically executed. It should be noted that a smart contract consists of a couple of declarative statements that may have logical connections. Therefore, once a condition is triggered, the connected statements are automatically executed and validated by blockchain miners. The verification and execution contract status is written on the blockchain.

2.1.4 Completion of a Smart Contract

After the evaluation of a smart contract, the status of the involved parties is updated. All the executed transactions and the updated states of all parties are written in the blockchain. Meanwhile, the involved parties transfer digital assets according to the contract policy. After the completion of digital asset transfer, the asset is unlocked, and it completed the life cycle of a smart contract.

It is to be noted that during the deployment and freezing, evaluation, and completion stage of a smart contract life cycle, a sequence of transactions is executed, written in the blockchain (see Fig. 2.3).

2.2 Blockchain Consensus Algorithms

If every node broadcasts blocks that hold verified transactions in a blockchain network, then confusion could arise. For instance, if we consider a verified transaction that needs to be inserted into the block and multiple nodes perform broadcasting about that, we can observe redundant transactions in different blocks. Thus, the ledger would be meaningless; rather than, a node needs to be selected that will be responsible for inserting the transaction into a block. After successfully inserting all the verified transactions into the block, the nodes within a blockchain network need to verify and reach an agreement (called *consensus*) to insert a new block to the main chain. Each participated node needs to prove its validity and authenticity before inserting a new block to the chain. The first node that is able to accomplish consensus will have the right to insert the new block. Once a block is verified and inserted into the chain, it is infeasible to modify or delete that block [8, 9]. We can achieve consensus in a blockchain network by applying various proof-based algorithm. In this section, we discuss various consensus models and how they actually work.

2.2.1 Proof-of-Work (PoW) Consensus Model

The most popular and widely used consensus mechanism is proof of work (PoW), which is used in Bitcoin. In currency cryptography, PoW has been a popular choice for many years. Under PoW, a participant is called a miner. The miners perform a computational task, i.e., solve a puzzle problem in order to obtain the right to generate a new block. The nodes perform puzzle solving by finding a specific hash function. Each blockchain miner tries to solve the hash value, i.e., they try to figure out a particular value as a nonce to meet a predefined hash condition, e.g., finding the nonce value that will make the first 30 bits of its hash to zero. The difficulty of the consensus mechanism can be increased by setting a hard puzzle. Each miner tries to find hash values that are smaller than or equal to a certain target value to reach consensus in the blockchain network [10, 11]. Whenever a miner finds the target hash value, it broadcasts the current block to the whole network. After that, all other nodes verify the correctness of its hash value. If the block is legit, all nodes append that new validated block to their blockchain. In Fig. 2.4, we presented an illustration of proof-of-work (PoW) consensus mechanism.

The main advantage of PoW is its strong security, an acceptable level of scalability, and decentralization feature. However, the block mining and validation

Fig. 2.4 Proof-of-work (PoW) consensus mechanism

process of PoW wastes a lot of energy. As more difficult the puzzle is, the more computational power is required. Therefore, the resource-constrained nodes would not solve a complex puzzle as the target hash generation time and success rate depend on the node's computational ability [12]. In summary, the disadvantages of PoW are high block creation time, high energy requirement, less throughput, and special hardware dependency.

2.2.2 Proof of Stake (PoS)

The next common and widely used distributed consensus algorithm is proof of stake (PoS). The main aim of creating PoS concept is to eliminate the main drawback of PoW, i.e., energy inefficiency. In PoS-based approach, the creator of next block is selected via different combinations of random selection, stake supply, and age that could provide scalability. The idea of PoS was first introduced in 2011, particularly for Peercoin cryptocurrency, and later on was used in others, i.e., Nxt and Blackcoin [13]. In this consensus mechanism, the node for creating next block is selected

via a quasi-random process, and the selection is performed by considering the assets stored in the wallets of the nodes. As this method does not require high computational power to validate any proof, the miners do not receive any reward without the transaction fees. The advantages of PoS are energy efficiency, high throughput, fast block creation time, scalability (less than PoW), and no dependence or requirement of special hardware of the nodes. Although PoS does not require computation power like PoW, it depends on the nodes that possess the most stake, and eventually, blockchain may become centralized. Another common problem of PoS is called "nothing at stake"; it means that if a node within a blockchain network has nothing in its stake while misbehaving, then the node would not be afraid of losing anything. Therefore, the node will not face any obstacle that prevents it from misbehaving within the network. One example of node misbehavior could be constructing two sets of new blocks to get double transaction fees [14, 15]. In Fig. 2.5, we presented an illustration of proof-of-stake (PoS) consensus mechanism.

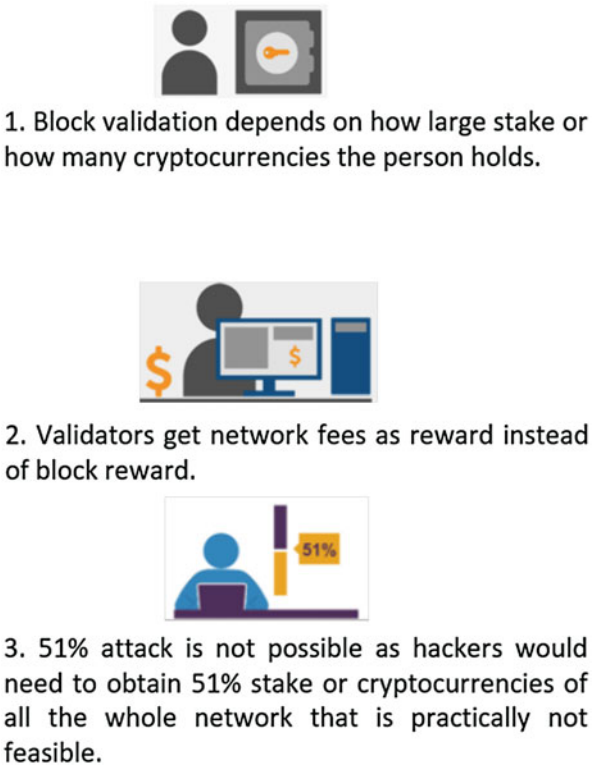

Fig. 2.5 Proof-of-stake (PoS) consensus mechanism

2.2.3 *Practical Byzantine Fault Tolerance*

Practical Byzantine fault tolerance (PBFT) is a replication algorithm that can tolerate Byzantine faults [16], inconsistency issues due to unreliable nodes within the system, and can perform efficiently than previous approaches [16, 17]. Today's malicious attacks on software can be an outcome of arbitrary or Byzantine behavior of faulty nodes. PBFT consensus algorithm is a formation of responsive machine code and used for solving such Byzantine general problems. In the PBFT method, all blockchain nodes must participate in voting to include the next block to the chain. The consensus is achieved if more than two-thirds of the blockchain nodes agree that the block and PBFT method withstand the remaining one-third nodes' opinion. Otherwise, consensus will not be achieved. In this way, PBFT achieves faster consensus and is comparatively more economical than PoW. Besides, the PBFT does not require any asset in the stake of the nodes for the consensus process [15]. In summary, PBFT has energy efficiency and high throughput that can be considered as its advantages. There remain possible delays as the blockchain network may need to wait to receive votes from all nodes, and the security scheme is not stronger than PoW. In Fig. 2.6, we presented an illustration of practical Byzantine fault tolerance (PBFT) consensus mechanism.

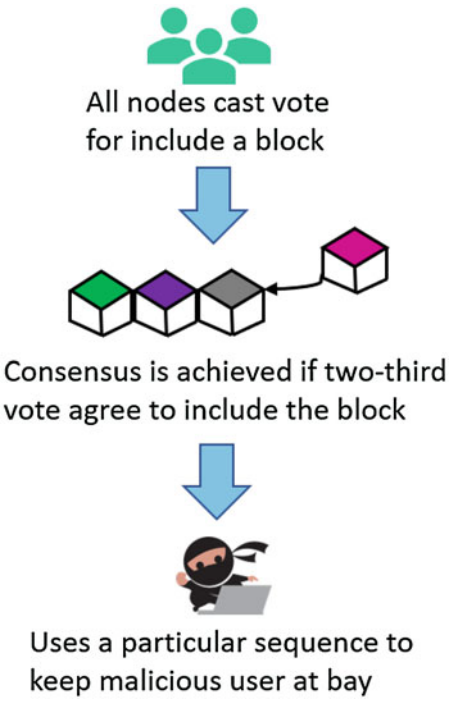

Fig. 2.6 Practical Byzantine fault tolerance (PBFT) consensus mechanism

2.2.4 *Proof of Elapsed Time*

Proof of elapsed time (PoET) is another consensus mechanism that uses a fair lottery protocol. Through fair lottery protocol, PoET consensus scheme prevents high energy consumption and high resource utilization by the blockchain nodes. This consensus algorithm uses a random elapsed time to choose nodes that are going to obtain mining rights and select block winners. Besides, PoET consensus mechanism improves transparency by certifying that lottery results of PoET protocol are verifiable by outsider or external participants. In summary, the workflow of PBFT is similar to PoW consensus algorithm without high power consumption of nodes. PBFT ensures power efficiency by allowing a blockchain miner to sleep and the nodes to switch to other tasks as per their convenience. In Fig. 2.7, we presented an illustration of proof-of-elapsed-time (PoET) consensus mechanism.

2.2.5 *Proof of Activity*

Another consensus algorithm is proof of activity (PoA), which is a hybrid consensus method that integrates both PoW and PoS. An example of PoA is Peercoin (PPC) that uses an initial PoW consensus mechanism combined with a PoS consensus. By integrating the PoW and PoS consensus mechanisms, a lower amount of energy is required, and the probability of 51% attack is also reduced. A 51% attack is basically a common attack on a blockchain network, where a single node or organization takes the control of the majority of the hash rate and causes disruption in the blockchain

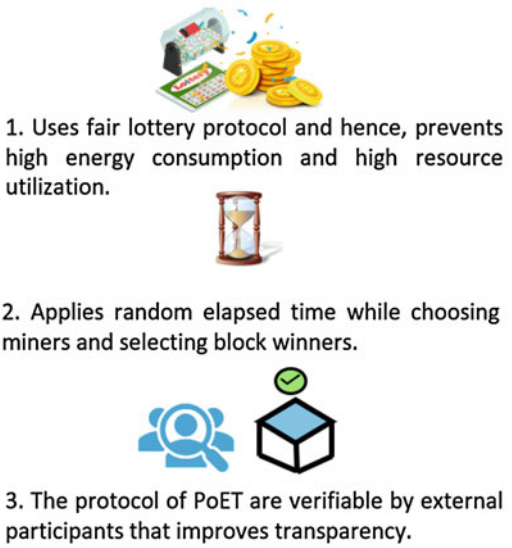

Fig. 2.7 Proof-of-elapsed-time (PoET) consensus mechanism

network. In such a situation, the attacker who grabs control over the majority hash rate can intentionally modify or exclude any transactions from the blockchain. The 51% attack problem is mostly seen in PoW consensus model, and PoA extensively reduces the chances of such an attack. In Fig. 2.8, we presented an illustration of proof-of-activity (PoA) consensus mechanism.

2.2.6 *Proof of Importance*

Proof-of-importance (PoI) consensus model is used to determine eligible users to perform necessary calculations while adding a new block to a blockchain and collecting associated payment. A PoI consensus model prioritizes blockchain miners by considering the value of coins it contains and the number of transactions they perform in their corresponding cryptocurrency. The more the transactions are made from the nodes' wallet, the higher the chances of being given to create the next block. In Fig. 2.9, we presented an illustration of proof-of-importance (PoI) consensus mechanism.

2.2.7 *Proof of Capacity*

The idea of proof of capacity (PoC) was first introduced in [18]. In this approach, the miners use free spaces of their hard disk for mining free coins. The algorithm comprises plotting hard drive of the nodes, i.e., performing computation and storing solutions on the hard disks before the block mining begins. The node that stores the fastest (closest) solution of the block puzzle wins the block. Using this protocol,

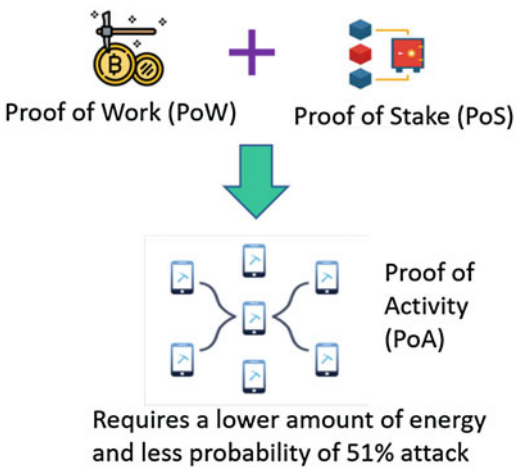

Fig. 2.8 Proof-of-activity (PoA) consensus mechanism

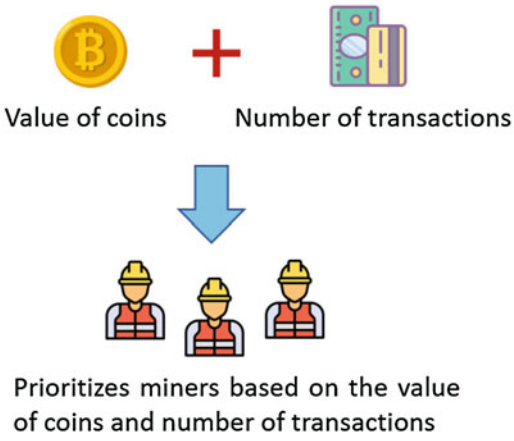

Fig. 2.9 Proof-of-importance (PoI) consensus mechanism

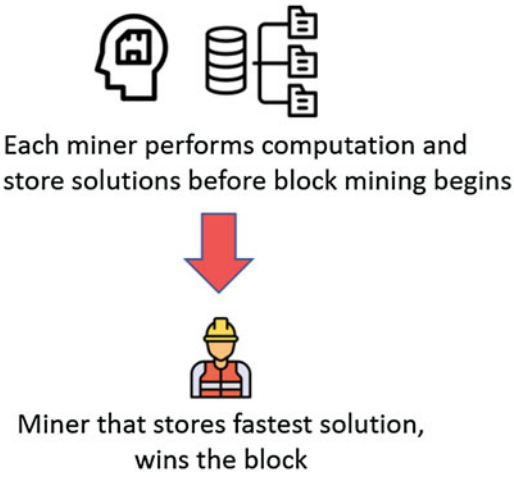

Fig. 2.10 Proof-of-capacity (PoC) consensus mechanism

the capacity of storage space of user's hard drive can be utilized. In this consensus model, the more space in hard drive a node has, the better chance to mine the next block and get reward. In Fig. 2.10, we presented an illustration of proof-of-capacity (PoC) consensus mechanism.

2.2.8 Proof of Burn

In proof-of-burn (PoB) consensus model, the blockchain nodes "burn" their coins, i.e., the nodes send their coins to an address from where the coins are irretrievable. By passing the coins toward a never–never land, each node gets a lifetime privilege to perform system mining through a random selection procedure [19]. Blockchain miners have a better chance and prioritize mining the next block as per the amount

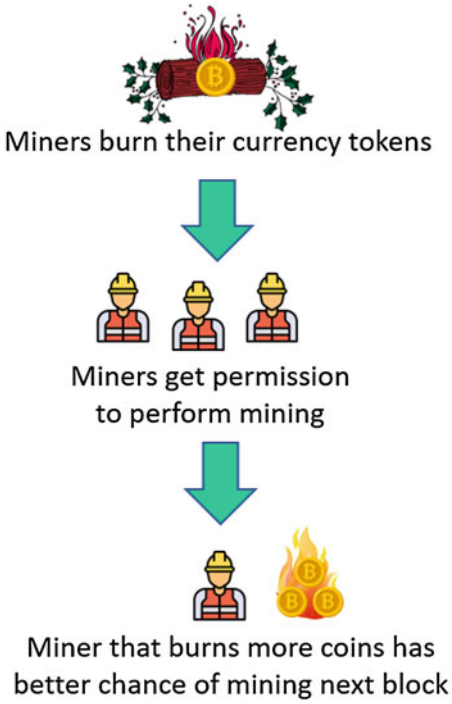

Fig. 2.11 Proof-of-burn (PoB) consensus mechanism

of coins they burn. In Fig. 2.11, we presented an illustration of proof-of-burn (PoB) consensus mechanism.

2.3 Comparison of Typical Consensus Algorithms

In this section, we compare the consensus algorithms that we discussed in Sect. 2.2 (Table 2.1). We compare the consensus algorithm based on accessibility, scalability, decentralization, throughput, and latency [15, 20, 21].

2.4 Discussion

This chapter covers the life cycle and a detailed working procedure of smart contracts in blockchain technology. We also explain various consensus algorithms, including their working process, and discuss what criteria are required while applying those consensus mechanisms in blockchain technology. To the end, we show a comparison table that highlights the core difference among those consensus algorithms.

Table 2.1 Comparison of consensus algorithms

Consensus method	Accessibility	Scalability	Decentralization	Throughput	Latency
PoW	Public, permissionless	High	High	Low	High
PoS	Public, permissionless, permissioned	High	High	Low	High
PBFT	Private, permissioned	Low	Medium	High	Low
PoET	Public, permissionless, permissioned	High	Medium	High	Low
PoA	Public, permissionless	High	High	Low	Medium
PoI	Public, permissionless	High	High	High	Medium
PoC	Public, permissionless	High	High	Low	High
PoB	Public, permissionless	High	High	Low	High

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Manubot (2019)
2. Szabo, N.: The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials 6 (1997)
3. Wikipedia Contributors: Smart contract, Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Smart_contract&oldid=983355857 (accessed October 29, 2020)
4. Dai, H.-N., Zheng, Z., Zhang, Y.: Blockchain for Internet of Things: A survey. IEEE Int. Things J. **6**(5), 8076–8094 (2019)
5. Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., Imran, M.: An overview on smart contracts: Challenges, advances and platforms. Future Gener. Comput. Syst. **105**, 475–491 (2020). https://doi.org/10.1016/j.future.2019.12.019
6. Idelberger, F., Governatori, G., Riveret, R., Sartor, G.: Evaluation of logic-based smart contracts for blockchain systems. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web, RuleML, pp. 167–183. Springer (2016)
7. Sillaber, C., Waltl, B.: Life cycle of smart contracts in blockchain ecosystems. Datenschutz und Datensicherheit-DuD **41**(8), 497–500 (2017)
8. Salimitari, M., Chatterjee, M.: A survey on consensus protocols in blockchain for iot networks. Preprint (2018). arXiv:1809.05613
9. Zhou, Q., Huang, H., Zheng, Z., Bian, J.: Solutions to scalability of blockchain: A survey. IEEE Access **8**, 16440–16455 (2020)
10. Xu, C., Wang, K., Guo, M.: Intelligent resource management in blockchain-based cloud datacenters. IEEE Cloud Comput. **4**(6), 50–59 (2017)
11. Wang, W., Hoang, D.T., Xiong, Z., Niyato, D., Wang, P., Hu, P., Wen, Y.: A survey on consensus mechanisms and mining management in blockchain networks. Preprint, 1–33 (2018). arXiv:1805.02707
12. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2017)

13. Bashir, I.: Mastering Blockchain. Packt Publishing Ltd. (2017)
14. Bach, L.M., Mihaljevic, B., Zagar, M.: Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1545–1550. IEEE (2018)
15. Salimitari, M., Chatterjee, M.: A survey on consensus protocols in blockchain for iot networks. Preprint (2018). arXiv:1809.05613
16. Bamakan, S.M.H., Motavali, A., Bondarti, A.B.: A survey of blockchain consensus algorithms performance evaluation criteria. Expert Syst. Appl. 113385 (2020)
17. Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., Kim, D.I.: A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access **7**, 22328–22370 (2019)
18. Dziembowski, S., Faust, S., Kolmogorov, V., Pietrzak, K.: Proofs of space. Paper presented at the Annual Cryptology Conference (2015)
19. Debus, J.: Consensus methods in blockchain systems. Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep (2017)
20. Chalaemwongwan, N., Kurutach, W.: State of the art and challenges facing consensus protocols on blockchain. In: 2018 International Conference on Information Networking (ICOIN), pp. 957–962. IEEE (2018)
21. Zamani, M., Movahedi, M., Raykova, M.: RapidChain: Scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931–948. ACM (2018)

Chapter 3
Blockchain Interoperability from the Perspective of Interdependent Networks

In this chapter, we discuss blockchain interoperability from the perspective of interdependent networks. At first, we define blockchain interoperability and present a high-level architecture view. After that, we discuss the design philosophy of blockchain interoperability that includes different interoperable blockchain considerations. Furthermore, we show a comparison of existing blockchain schemes. To the end, we present open issues with challenges and highlight some research directions on the blockchain interoperability domain (Fig. 3.1).

3.1 Interoperability Definition

Next generation blockchain systems will be powered by large and distinct blockchain networks. Such systems would need to enable cross-chain mechanisms to improve capabilities and upgrade functionalities in the future landscape. *Blockchain Interoperability* holds the same theme by enabling multiple blockchains to work together. A classic blockchain $\mathcal{B}_1$ allows a transaction when it maintains the $\mathcal{B}_1$'s rules considering the present state of $\mathcal{B}_1$. In the same way, a blockchain $\mathcal{B}_1$ is interoperable with another chain $\mathcal{B}_2$ and accepts transactions if that transaction does not transgress the rules.

Definition (Blockchain Interoperability) Let $\mathcal{B}_1 = (\mathcal{L}_{\mathcal{B}_1}, \mathcal{S}_{\mathcal{B}_1}, \text{Emission}_{\mathcal{B}_1}, \text{Mining}_{\mathcal{B}_1}, \text{Consensus}_{\mathcal{B}_1})$ and $\mathcal{B}_2 = (\mathcal{L}_{\mathcal{B}_2}, \mathcal{S}_{\mathcal{B}_2}, \text{Emission}_{\mathcal{B}_2}, \text{Mining}_{\mathcal{B}_2}, \text{Consensus}_{\mathcal{B}_2})$ be two blockchains. Let δ_{B_1} and δ_{B_2} be two sets that contain all possible values for the ledgers of $\mathcal{L}_{B_1}$ and $\mathcal{L}_{B_2}$, respectively. Now, blockchain $\mathcal{B}_1$ is regarded as interoperable with blockchain $\mathcal{B}_2$ if there exist

- a transaction $t \in \mathcal{T}$,
- a non-empty subset $\omega_{\mathcal{B}} \subset \delta_{\mathcal{B}_1}$, and $\omega_B \subsetneqq \delta_{B_2}$ and

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_3

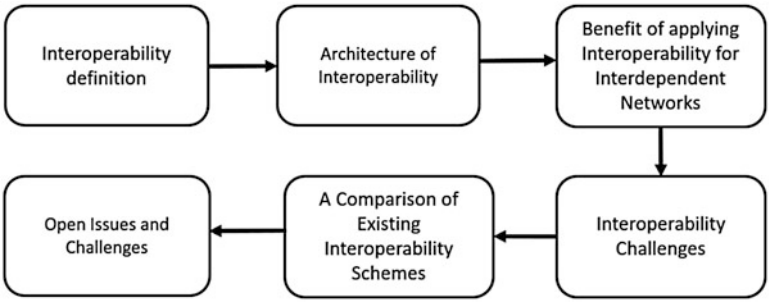

Fig. 3.1 Chapter overview

- there exists such a block that contains transaction t, which is accepted by Consensus_{B_1} if $\mathcal{L}_{\mathcal{B}_1} \times \mathcal{L}_{\mathcal{B}_2} \in \omega_{\mathcal{B}_1} \times \omega_{\mathcal{B}_2}$, and otherwise, rejected.

3.2 An Architecture of Interoperability

The architecture of interoperability needs to be constructed in such a way so that security, traceability, and irreversibility are ensured in all the participated chains. For convenience, we can consider two chains (e.g., a blockchain for an energy network and another one for a transportation network) that wish to share data and exchange information. The chain that shares data is called source chain, and the receiver is called the destination chain. Suppose we enable interoperability by reading from the source chain and writing on the destination chain further. In that case, there may be a security concern for such an indirect interaction as the notary may tamper the shared data. As a result, the effectiveness of the interoperability can be degraded. To resolve the issue, a direct interaction paradigm can be effective for interoperability, which is presented in Fig. 3.2. In such a paradigm, data can be retrieved and transferred between two blockchains (that may reside in different blockchain networks, e.g., transportation, energy, water, or financial networks [1]) without any notary for maintaining effective performance and security of the blockchain ecosystem. Therefore, interoperability can be regarded as an intelligent characteristic that allows direct information exchange from one chain to another while preserves the essence of the participated blockchains. The cross-chain framework generally consists of five layers that work together to handle the issues related to interoperability, which are discussed below.

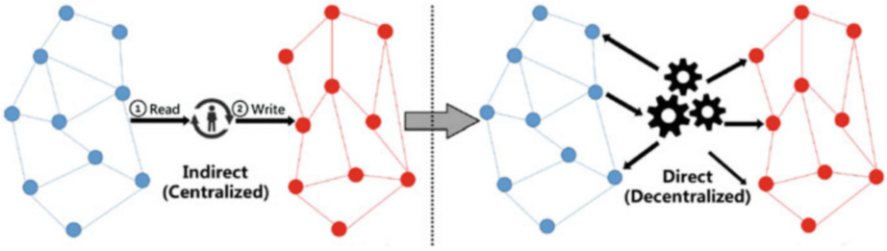

Fig. 3.2 A high-level architecture of blockchain interoperability [2]

3.2.1 Data Generation in Data Layer

One of the most important tasks in blockchain systems is to manage data that includes maintaining block structure, transaction format, modeling storage, etc. Blockchain systems may vary in terms of the data layers, and diverse transaction format is one of the bottlenecks for enabling information exchange across multiple blockchains. For instance, the data format of Bitcoin and Ethereum is not similar that results in impediments while making a transaction between Bitcoin and Ethereum. One possible solution is to create a unified transaction format that is facilitated by the data generator module. A middleware can be built with a data generator that allows direct interaction among multiple blockchains. The blockchain ecosystems can easily adapt the unified transaction format and make a connection with the middleware. However, there would add more complexity if we change each existing blockchain's transaction format, rather than a transaction translator can help translate the transactions from a blockchain's specific format to a unified one.

3.2.2 Cross-Chain Mechanism in Network Layer

The main purpose of the network layer in the blockchain is to maintain communication among available nodes. To leverage the decentralization nature and carry out intra-blockchain communication, P2P protocol, gossip protocol, or a combination of P2P and gossip protocols is widely used. Besides, a cross-chain communication mechanism is proposed by [2] to enable inter-blockchain communication for ensuring interoperability. However, the cross-chain communication may arise several issues, i.e., discovering IP address of the counter blockchain without presence of any trusted authority or centralized server, obtaining notable performance, handling of consensus mechanism of the communicated blockchains.

3.2.3 Verification of Transaction in Consensus Layer

Another essential stage of blockchain interoperability is to verify the transaction in order to ensure the consistency of blockchain states. The consensus algorithms can be classified into two categories: Nakamoto consensus, which includes proof of work (PoW), proof of stake (PoS), proof of elapsed time (PoET), proof of location (PoL), etc. and classical consensus such as practical Byzantine fault tolerance (PBFT). During cross-chain communication, the consensus algorithms examine whether valid data is committed and shared from the source chain. Besides, the consensus algorithms can verify whether data has been tampered or not on the destination chain.

3.2.4 Smart Contract for Cross-Chain Mechanism in Contract Layer

To enable cross-chain communication between multiple blockchains, there needs to be constructed a smart contract that would hold all the transaction rules, policies, and agreements. That smart contract needs to be prepared on the consent of the participated nodes from the communicated blockchains. The smart contract would be triggered during a transaction between source and destination blockchains. However, the main challenge is to consider a unified programming language and runtime environments for source and destination blockchains since different blockchains may be constructed with different programming languages and runtime environments.

3.2.5 Application Programming Interface (API) in Application Layer

Finally, the interface for performing interoperability among multiple blockchains should be user-friendly. Many developers get interested in taking part in the developing process, and users can easily carry out the interoperable actions with other blockchain networks.

3.3 How Blockchain Interoperability Concept Can Be Useful for Interdependent Networks?

In a conventional system, networks are studied in an individualistic manner. With the ever-improvements of related technologies, the coupling of different networks has

become a feasible task. Interdependent networks mean the dependency of different networks to execute their regular operations. For instance, transportation networks may need to know about the demand response status of a particular city that could be provided by energy networks. Similarly, water has direct relation with energy networks, or a financial network may perform necessary operations after exchanging information with energy networks. Now, suppose we apply blockchain for such interdependent networks. In that case, we need to apply blockchain interoperability that allows us to exchange data among multiple blockchains that may be different in architecture, protocols, consensus mechanism, and so on. Without enabling blockchain interoperability, data would be restricted only in a single chain; thus, the main theme of interdependent networks (i.e., sharing data) would not be achieved. However, enabling blockchain interoperability is not a straightforward task. Several technical challenges would arise while applying blockchain interoperability for interdependent networks, and we discuss those challenges in our next section.

3.4 Interoperability Challenges

The goal of establishing interoperability is not an easy task. Several challenges arise while applying interoperability across multiple chains: assurance of atomicity, security maintenance, improvement of efficiency, tolerance of diversification, and user-friendliness. However, there is no universal framework that can solve all the stated issues.

3.4.1 Assurance of Atomicity

The guarantee of atomicity for blockchain interoperability event is a challenging task. For interoperability, atomicity means any event that performs on the chains needs to be either completely successful or unsuccessful at the same time for both chains. For instance, we can consider two different financial companies (namely, A and B) that possess different blockchains and they try to transfer assets. A customer from company “A” named “X” wants to send some assets to a customer named “Y” from company “B.” Now, if customer “X” transfers money to customer “Y,” then customer “X”’s assets on chain “A” should decrease, while customer “y”’s asset on chain “B” should increase. Both of these events should be either successful or unsuccessful for a particular event.

3.4.2 Improvement of Efficiency

Blockchain interoperability is always challenging to maintain a stable cross-chain communication and accelerate the data exchange process. The interoperability process's performance affects multiple parties; hence, it deserves more attention to ensure a swift cross-chain operation. The efficiency can be accessed and determined by examining the chain interaction times in every second. The consensus mechanism that includes transaction validation, data commitment speed at the destination chain, effective cross-chain communication, smart contract, and verification module are regarded as the essential factors for improving blockchain interoperability.

3.4.3 Maintenance of Security

The cross-chain mechanism raises the security risks that could subvert the blockchain ecosystem's security. The cross-chain mechanism introduces more security risks than individual blockchain operations. The data transmission process of the cross-chain process has three phases: (1) the shared data is leaving the source chain, (2) the shared data leaves source chain and currently in transit, and (3) the shared data is reaching at the destination chain. These phases result in the necessity of undertaking different measures to consider for each phase. In particular, the security maintenance across multiple chains needs to satisfy the following: (a) the shared data collects from a random node, needs to commit on the source chain, and should be reliable, (b) the shared data while in transit cannot be tampered, and a signature checking mechanism can be incorporated, and (c) a final commitment should be encountered on the destination chain after the shared data reaches to the destination chain without any temperament.

3.4.4 Handling of Diversification

During blockchain interoperability, we may face diversification in terms of a consensus protocol or usage scenarios. The consensus mechanism of a company "M"'s blockchain may be distinct from the consensus of another company "N"'s blockchain due to their diverse business policies. Besides, several open-source blockchain source codes are available that could be customized by making some code changes, and it brings diversity in the usage scenarios within blockchain systems. That means very few changes are required when a new blockchain joins the blockchain ecosystems and the blockchains try to exchange information.

3.5 A Comparison of Existing Interoperability Schemes

A few interoperability schemes are available that vary in terms of interoperability, atomicity, universality, efficiency, and security. In Table 3.1, we present the comparison of some of the existing blockchain interoperability schemes.

3.6 Open Issues and Challenges

This section discusses the open issues and challenges related to blockchain interoperability, i.e., the adaptation of communication and data exchange mechanisms among multiple blockchains. It is challenging to ensure correct executions on a different blockchain without the presence of any trusted authority. Although notable recent advancement is made, there is still a marginal gap between theory and practical aspects in the blockchain interoperability domain.

It is not easy to coordinate different blockchain transactions to support cross-chain communication, as blockchains may vary in terms of architecture, access controls, protocols, and service discovery. Besides, it is complicated to revert a transaction that depends on another, particularly when transaction decisions are made in different blockchains. Although some solutions (e.g., [6]) toward this issue are proposed, they are still not rigorous to be applied in a complex cross-chain decentralized application (dApp). More extensive research is necessary to handle the issue effectively.

Some prior works (e.g., [7]) discussed problems regarding security, confidentiality, trust, and data privacy issues. These issues are exacerbated during the collaboration of multiple blockchains with their respective properties. Regarding privacy, if a user asks for the deletion of their shared personal data, there are no effective mechanisms to respond to that request. To minimize the leakage and confidentiality, blockchain fine-grained access control [8, 9] can be adapted. Furthermore, blockchain interoperability raises the risk of attacks [10, 11] due to variant access control, consensus algorithms, protocols, or service discovery in underlying cross-chain communication. In a nutshell, the most prominent open issues and challenges in blockchain interoperability areas are security and privacy [12–14], discoverability [15], and governance [16, 17].

Table 3.1 Comparison of existing blockchain interoperability schemes

Approach	Atomicity	Interoperability	Universality	Efficiency	Security
Notary [3]	Good	Medium	Poor	Good	Poor
Sidechains [4]	Good	Medium	Poor	Poor	Good
Hash-locking [5]	Good	Medium	Poor	Poor	Good
MMR [2]	Good	Good	Medium	Good	Good

3.7 Research Directions

For smooth operations of blockchain interoperability, new frameworks, protocols, and programming models are in the emerging process and still need further development. While protocols (e.g., UIP, ILP) enable cross-chain transactions, Cosmos [18] and Polkadot [19] programming models allow developers to create blockchain and make communication with other blockchain networks. However, if the communicated blockchain types (i.e., private, public, permissioned) are different, we may face trouble performing cross-chain communication. A few solutions are proposed in this regard, e.g., multichain [20] can connect to Bitcoin but has limited functionalities. Therefore, bidirectionally connecting various types of blockchains is an open research problem. In the light of prior research and identification of open research issues and challenges, we point out research directions on blockchain interoperability domain considering blockchain architecture, cryptocurrency, blockchain engines and connectors, tools, standards, programming languages, and others.

Blockchain Interoperability Design

- Designing an effective blockchain interoperability model by considering various levels of interoperability layers, e.g., technical layers that consider technical factors to integrate blockchains, and semantic layers that are concerned with preserving application-specific semantics across blockchains.
- Modeling different views based on interoperability types and stakeholders, e.g., technical view for provider on a dApp vs. semantic view for end user on the same dApp.

Managing Cryptocurrency for Blockchain Interoperability

- Developing protocols for allowing authorized money exchange.
- Improving level of security and privacy during decentralized cryptocurrency exchange.
- Developing solutions with the aim of obtaining optimal benefit from side chains for permissioned blockchains.

Blockchain Engines

- Developing blockchain engines to bridge permissioned blockchains with permissionless blockchain to evaluate effective interoperability for various blockchain types.

Blockchain Connectors

- Study how the trust of trusted parties that route transactions from source to a destination blockchain can be made decentralized and integrate with a public blockchain, i.e., periodically acknowledging the state to a public blockchain.
- Guarantee atomicity on cross-blockchain dApps.
- Improving consistency and integrity during cross-blockchain communication.

- Constructing blockchain migration schemes for permissioned and public ledgers by considering various functionalities set by stakeholders.
- Coupling newly developed blockchain engines with existing blockchain systems.

Supporting Tools, Standards, and Programming Languages

- Developing new tools, standards, programming languages, frameworks, and verifiable credentials for cross-blockchain mechanisms.
- An extensive study on security loopholes of blockchain interoperability.
- Examining the effectiveness of integrating cryptocurrency schemes, blockchain engines, and connectors for cross-chain decentralized applications.

3.8 Discussion

This chapter presents the blockchain interoperability concepts by presenting details about the cross-chain architecture and its layers. We discuss the importance of applying interoperability in interdependent networks and possible challenges in deploying cross-chain communication among multiple blockchains. Furthermore, we provide a comparison of existing blockchain schemes. To the end, we highlight the open issues and challenges considering the prior works and point out the research directions in blockchain interoperability domains from the perspective of interdependent networks.

References

1. Amini, M.H., Imteaj, A., Pardalos, P.M.: Interdependent networks: A data science perspective. Patterns **1**(1), 100003 (2020)
2. Jin, H., Dai, X., Xiao, J.: Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1203–1211. IEEE (2018)
3. Hegnauer, T.: Design and Development of a Blockchain Interoperability API. Ph.D. diss., Master's thesis, CSG@ IFI, University of Zurich, Switzerland, to appear 2019. Supervisors: Eder Scheid, Bruno Rodrigues, Burkhard Stiller, 2019
4. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains, vol. 72 (2014). https://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains
5. Deng, L., Chen, H., Zeng, J., Zhang, L.-J.: Research on cross-chain technology based on sidechain and hash-locking. In: International Conference on Edge Computing, pp. 144–151. Springer, Cham (2018)
6. Besançon, L., Da Silva, C.F., Ghodous, P.: Towards blockchain interoperability: Improving video games data exchange. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 81–85. IEEE (2019)
7. Hoang Tam, V., Wang, Z., Karunamoorthy, D., Wagner, J., Abebe, E., Mohania, M.: Internet of blockchains: techniques and challenges ahead. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)

and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1574–1581. IEEE (2018)
8. Wang, S., Zhang, Y., Zhang, Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access **6**, 38437–38450 (2018)
9. Lin, C., He, D., Huang, X., Raymond Choo, K.-K., Vasilakos, A.V.: BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J. Network Comput. Appl. **116**, 42–52 (2018)
10. Sai, K., Tipper, D.: Disincentivizing double spend attacks across interoperable blockchains. In: 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 36–45. IEEE (2019)
11. Borkowski, M., Sigwart, M., Frauenthaler, P., Hukkinen, T., Schulte, S.: DeXTT: Deterministic cross-blockchain token transfers. IEEE Access **7**, 111030–111042 (2019)
12. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Informatics **36**, 55–81 (2019)
13. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
14. Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J.A., Liu, R.P.: Survey: Sharding in blockchains. IEEE Access **8**, 14155–14181 (2020)
15. Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., Hu, Y.-C.: Hyperservice: Interoperability and programmability across heterogeneous blockchains. In: ACM SIGSAC Conference on Computer and Communications (2019)
16. Hardjono, T., Lipton, A., Pentland, A.: Towards a public key management framework for virtual assets and virtual asset service providers. http://arxiv.org/abs/1909.08607
17. Hardjono, T., Lipton, A., Pentland, A.: Toward an interoperability architecture for blockchain autonomous systems. IEEE Trans. Eng. Manag. **67**(4), 1298–1309 (2019)
18. Cosmos Network: https://cosmos.network, Accessed 2019
19. Wood, G.: Polkadot: Vision for a heterogeneous multi-chain framework. White Paper (2016)
20. Greenspan, G.: MultiChain White Paper (2015). https://www.multichain.com/white-paper/

Part II
Blockchain Applications

Chapter 4
Blockchain Applicability in Internet-of-Things (IoT) Environment

This chapter introduces the importance of designing IoT applications that deploy blockchain technology. We discussed when we should choose to apply blockchain technology for an IoT and highlighted some existing blockchain-based IoT (BIoT) applications. To this end, we analyzed some current challenges of BIoT applications and presented some further challenges and recommendations. In Fig. 4.1, we illustrated the high-level overview of this chapter.

4.1 Importance of Integrating Blockchain with IoT

The author in [1] proposed an idea of shifting toward a decentralized paradigm for the fast-growing IoT ecosystem to ensure sustainability. The conventional centralized IoT device ecosystem encounters high communication costs while making a decision. If we consider a smart manufacturing system, then the current centralized based IoT approach would result in a high maintenance cost, e.g., release and distribute a software update to thousands of devices. Besides, IoT-based systems have a high probability of containing vulnerable and malicious devices that could affect the data collection and decision-making process. Blockchain facilitates a trustless, scalable peer-to-peer model that ensures transparency and secure distribution of data. The unique characteristics of IoT impose several research challenges in the following domains:

- Heterogeneity: The heterogeneity of IoT-based systems means the variation of IoT network in terms of devices and their capabilities, communication protocols, or data types (i.e., unstructured, structured, and semi-structured). The heterogeneity is also responsible for other major challenges such as privacy, security, and interoperability.
- Communication protocols: Variant network or communication protocols can coexist in IoT that may hold different network services, i.e., some protocol may

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_4

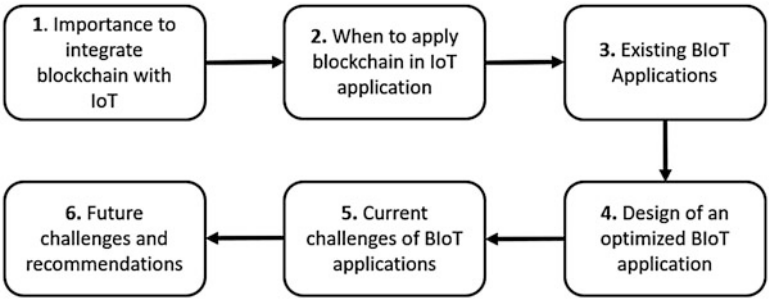

Fig. 4.1 Chapter overview

hold short communication coverage (e.g., not more than 100 m), while other may provide a long range of coverage, (e.g., 1–10 km) [2–4].

- Interoperability: Interoperability means IoT networks' capability to exchange and collaborate with each other to obtain additional and required information. Due to IoT systems' heterogeneity and decentralization, it becomes difficult to exchange data among different IoT networks.
- Resource limitations: The IoT devices may have limited resources in terms of bandwidth, battery life, memory, and processing capability. The resource-constrained behavior of the IoT devices makes them prone to malicious attacks.
- Privacy: Privacy preservation is the technique of ensuring proper usage of IoT data and information, i.e., not disclose anything without user consent. It is challenging to preserve IoT systems' privacy due to their structural complexity, decentralization scheme, heterogeneous devices, and limited resources. Besides, the integration of cloud computing with IoT systems provides additional processing and computing capabilities. However, the passing of IoT data to a third party may open up the door of privacy leakage.
- Security: The heterogeneity, resource limitations, and decentralization characteristics of IoT devices also result in a security vulnerability. The typical solutions of ensuring security may not be applicable for a resource-constrained IoT-based system due to the security countermeasures. Furthermore, IoT systems may also face different vulnerable attacks due to the inability to update security firmware with their limited resources [5, 6].

4.2 Customized Application of Blockchain in an IoT Environment

Before considering to integrate blockchain for an IoT application, we need to ensure that it is the best solution for that application. It is to be noted that blockchain is not suitable for all IoT scenarios. In order to determine whether a blockchain is necessary for an IoT application, we need to check the following features presented in Fig. 4.2:

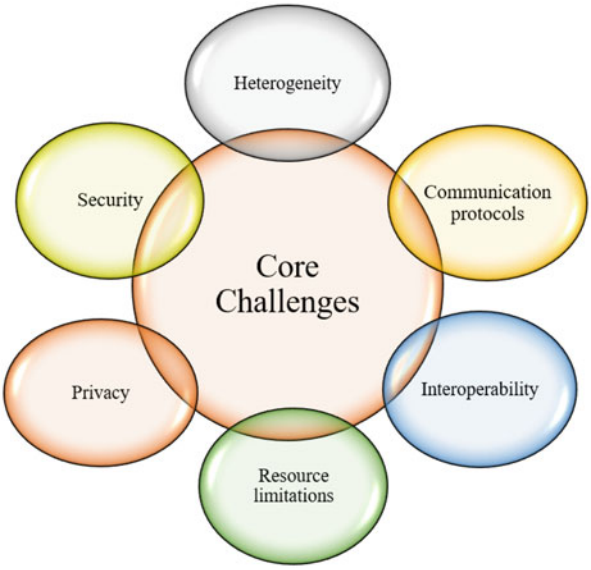

Fig. 4.2 Key challenges of integrating blockchain with IoT applications

- Decentralization: We need to establish decentralized feature for an IoT system when the central coordinator is not trustworthy. However, if the IoT systems' users can fully trust the central coordinator, then there is no need to integrate blockchain.
- Secured transactions: Sometimes, it may require IoT applications to perform transactions among the existing IoT nodes or third parties. During a transaction, atomicity should be ensured so that both parties of the transactions are guaranteed to receive their desired asset. In such a situation, blockchain can be adapted for IoT systems.
- Immutability: In a real-life IoT system, the IoT devices' extracted data and transaction history can be changed through malicious activities. In such a situation, if there is a need to ensure the immutability of the local data within IoT device, or cloud server, then we can integrate blockchain that holds the unique characteristic of enabling immutability within IoT systems.
- Timestamped sequential logging: It is required in some IoT applications to collect data by labeling with proper timestamp and store those sequentially. For those applications, we can apply blockchain to construct a timestamped sequential logging.
- Peer-to-peer exchanges: Most communications within IoT networks occur from nodes to gateways, i.e., the IoT devices pass data to the remote central server. However, the interaction among peers is not very common and may be required in some specific applications, e.g., intelligent swarms [7]. In such applications, blockchain can enable peer-to-peer secure interaction to achieve application goal.
- Storing microtransactions: Some IoT applications (e.g., [8, 9]) may need to track every record of transactions for auditing or maintaining traceability. In such

cases, a sidechain can be effective that can enable traceability of all transactions within the IoT networks.

In Fig. 4.3, we present a flow diagram that helps to determine when we should integrate blockchain within an IoT system.

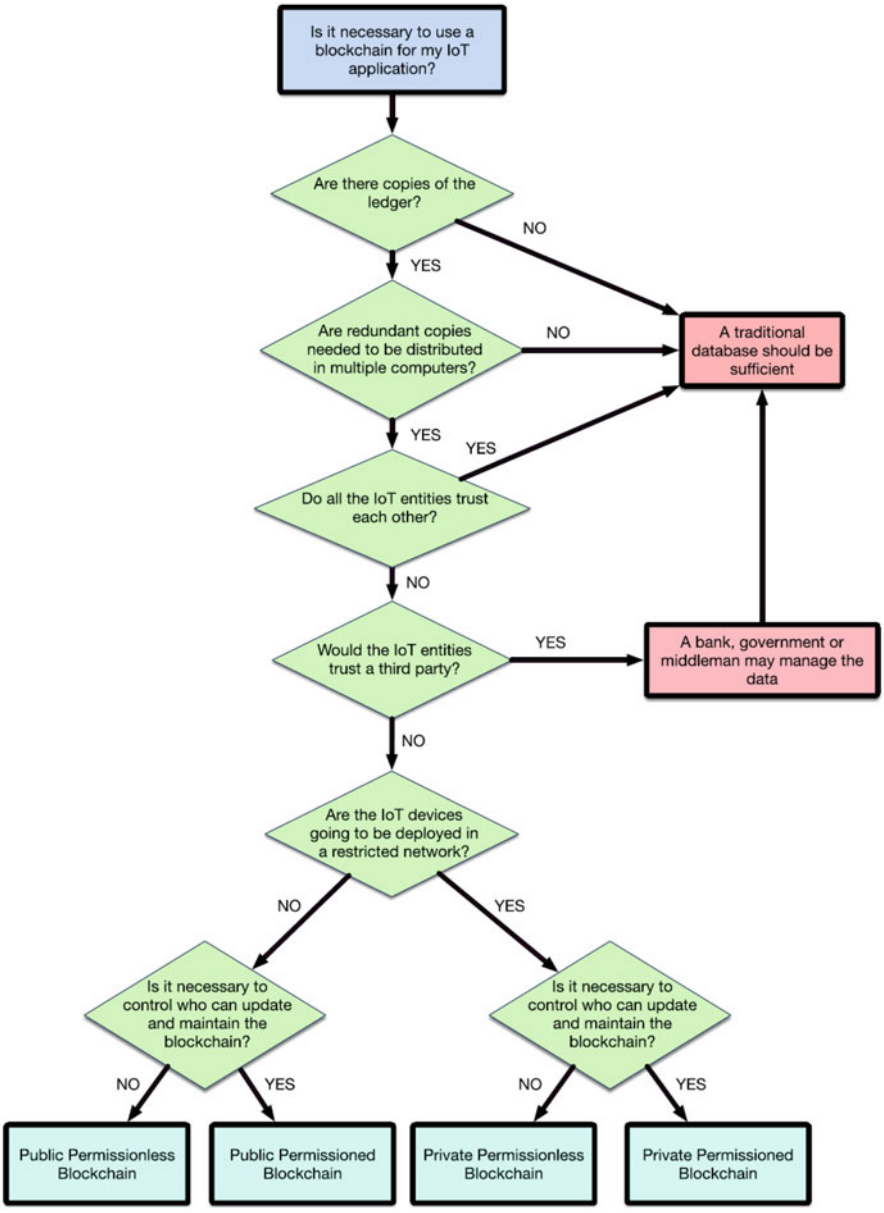

Fig. 4.3 Flow diagram to understand when to integrate blockchain within an IoT application [10]

4.3 Blockchain-Based IoT (BIoT) Applications

It is possible to integrate blockchain technology in several IoT applications (see Fig. 4.4). According to [11], the applicability of blockchain started with Bitcoin, after that shifted to smart contracts, and finally, evolved toward efficiency, atomicity, and coordination-based applications.

4.3.1 Smart Home

Blockchain can be served for various purposes on IoT-enabled smart home systems. Nowadays, smart homes are controlled and monitored with different smart sensors and devices that can capture events and perform necessary actions accordingly. However, the devices are prone to attacks and can reveal user sensitive information while passing data to a central server. Any slight modifications of any of the devices within a smart home then can cause a great loss. For instance, a smart lock that only opens the door of a smart home in the owner's presence can open that for an unknown person due to certain modifications within the device action rules. To ensure integrity, the security and privacy leakage in smart home management system can be handled with blockchain-based security access control [12], consensus mechanism [13], or secure blockchain architecture [14].

4.3.2 Smart Energy

Blockchain can be applied in the energy sector by allowing the devices to help each other in services without involving any human intervention [15]. The concept of distributed energy resource management scheme is reshaping consumers'

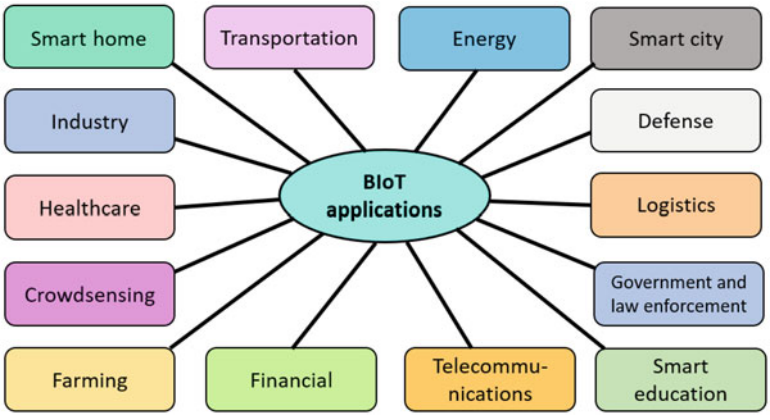

Fig. 4.4 Examples of existing BIoT applications

characteristics from consumer toward energy prosumers, i.e., can also contribute in generating energy in addition to consuming. The prosumers who have extra energy resources can sell to other consumers to receive some incentives. However, the energy trading is highly insecure if there is no trusted coordinator as the contract deal can be changed or any of the parties can disagree on their previous agreement. Considering the demand response energy trading market, the author in [16] proposed a blockchain-enabled energy trading market scheme and discussed how blockchain technology could ensure asset exchange immutable smart contract. Besides, the authors in [17] discussed an application to automatically pay for the electricity bill by connecting a smart cable to a smart socket. Moreover, a secure and transparent decentralized energy trading management system with blockchain technology for smart grid is proposed in [18]. Through their work, they demonstrated how energy trading transactions could be performed securely by coupling blockchain with IoT for smart grids.

4.3.3 Smart Healthcare

Healthcare sector can be immensely benefitted from blockchain technology. The recent advancements of wearable healthcare technologies open up the opportunities of providing remote healthcare services. This can be potentially effective when a hospital has limited human resources and a shortage of other resources (e.g., hospital cabin). Particularly, senior citizens can easily get remote healthcare services by staying at their houses and wearing the necessary wearable devices. The hospital authorities can check the continuous data streams from the corresponding wearable devices, e.g., blood sugar level, heart rate, blood pressure readings. However, it is important to preserve the integrity and accessibility of those sensitive data so that no one can misuse or tamper with any of the patient's data. Besides, the vulnerability of wearable devices and the heterogeneous nature of healthcare networks should also be checked to preserve patient privacy and security. The integration of blockchain in such IoT-enabled healthcare systems can limit the access of those sensitive data and ensure the immutability of such sensitive data. Moreover, blockchain-enabled clinical trials and making precision of appropriate medicine according to the patient's conditions are some useful BIoT applications [19].

4.3.4 Supply Chain Management

In a supply chain management system, a product can consist of multiple parts that can be supplied by different manufacturers. However, it is possible that some fraudulent low-quality parts are shipped into the supply chain, and it is expensive to check each product quality using advanced technologies. The coupling of blockchain and IoT can give a feasible and inexpensive solution for this problem. We can label each part of a product with a unique ID and an immutable timestamp

during their production. After that, each product–part identification is stored within a blockchain that is traceable and tamper-resistant. In this way, no fraudulent part can be shipped to the main product manufacturer.

Furthermore, BIoT applications can be applied in many sectors, including smart living applications [20, 21], sensing [22, 23], intelligent transportation [24], identity management [25], cyber law [26], mobile crowd sensing [27, 28], supply chain [29], or security missions [30, 31].

4.4 Current Challenges of BIoT Application

Dorri et al. [32] the emerging technologies that are based on IoT ecosystem such as telemetry systems [33], cyber-physical systems (CPS) [34], 4G/5G communications [35], and RFID [36] face several challenges in their operations. Though the integration of blockchain can improve the overall security and privacy, the construction of a BIoT application is a complicated process and many aspects are related with that. In this section, we describe the main factors that are responsible for arising challenges in BIoT applications.

- As IoT devices are resource constrained in nature, therefore, integrating blockchain technology may require more energy to perform additional task requirements, and optimizing the energy efficiency for BIoT applications is a challenging task.
- A BIoT application may need to manage a large amount of transactions every second. However, Bitcoin can only handle seven transactions per second, which can be further increased by changing certain aspects or considering larger blocks [37]. The different stages of the blockchain (e.g., consensus mechanism, block verification, and validation) encounter less throughput and increase latency.
- The blockchain size is another issue of BIoT applications. As the number of transactions increases, it requires a larger blockchain size to store those transactions. However, mining a large size of blockchain may require more resources, which would be difficult for IoT devices.
- The interoperability among different IoT networks is necessary to exchange information or carry out transactions. However, the access policy within smart contract can vary from one IoT system to another. Thus, it is challenging to leverage the interoperability feature in BIoT applications.
- Sometimes, blockchain is forked due to versioning or administrative purposes, and it may become difficult to carry out transactions among different chains once a blockchain is forked.
- As the blockchain miners decide which transactions should be stored within the blockchain and which should be avoided; therefore, if most miners (at least 51%) are malignant, they can influence certain transactions for ideological or economic reasons. Thus, choosing the appropriate miners for the BIoT applications is essential, and it is challenging to identify the misbehaved miners.

4.5 Discussion

In this chapter, we discussed the benefit of applying blockchain technology in different IoT applications. While the data at the edge devices are booming due to the recent advancement of IoT devices and internet facilities, the concerns related to the security, privacy, consistency, integrity, and immutability of data can be tackled by integrating blockchain with the IoT systems. By explaining the importance of coupling blockchain with IoT, the situation to apply blockchain in an IoT-based system, the existing BIoT applications, and the core challenges of implementing BIoT applications, we present a clear understanding of blockchain applicability within an IoT environment.

References

1. Brody, P., Pureswaran, V.: Device democracy: Saving the future of the Internet of Things. IBM Institute for Business Value, Technical Report 2014. Available: http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/
2. Dai, H.-N., Zheng, Z., Zhang, Y.: Blockchain for internet of things: a survey. IEEE Int. Things J. **6**(5), 8076–8094 (2019)
3. Chen, M., Miao, Y., Hao, Y., Hwang, K.: Narrow band internet of things. IEEE Access **5**, 20557–20577 (2017)
4. Khutsoane, O., Isong, B., Abu-Mahfouz, A.M.: IoT devices and applications based on LoRa/LoRaWAN. In: IECON 2017–43rd Annual Conference of the IEEE Industrial Electronics Society, pp. 6107–6112 (2017)
5. Roman, R., Zhou, J., Lopez, J.: On the features and challenges of security and privacy in distributed internet of things. Comput. Netw. **57**(10), 2266–2279 (2013)
6. Douglas, A., Holloway, R., Lohr, J., Morgan, E., Harfoush, K.: Blockchains for constrained edge devices. Blockchain: Res. Appl. **1**(1–2), 100004 (2020)
7. Gui, T., Ma, C., Wang, F., Wilkins, D.E.: Survey on swarm intelligence based routing protocols for wireless sensor networks: An extensive study. In: Proceedings of the IEEE International Conference on Industrial Technology (ICIT), Taipei (2016), pp. 1944–1949
8. Lomotey, R.K., Pry, J., Sriramoju, S., Kaku, E., Deters, R.: Wearable IoT data architecture. In: Proceedings of the IEEE World Congress on Services (SERVICES), Honolulu, pp. 44–50 (2017)
9. Wu, Z., Meng, Z., Gray, J.: IoT-based techniques for online M2Minteractive itemized data registration and offline information traceability in a digital manufacturing system. IEEE Trans. Ind. Informat. **13**(5), 2397–2405 (2017)
10. Fernández-Caramés, T.M., Fraga-Lamas, P.: A review on the use of blockchain for the internet of things. IEEE Access **6**, 32979–33001 (2018)
11. Swan, M.: Blockchain: Blueprint for a New Economy, 1st edn. O'Reilly Media, Newton (2015)
12. Xue, J., Xu, C., Zhang, Y.: Private blockchain-based secure access control for smart home systems. KSII Trans. Int. Inf. Syst. **12**(12), 6057–6078 (2018)
13. Singh, P.K., Singh, R., Nandi, S.K., Nandi, S.: Managing smart home appliances with proof of authority and blockchain. In: International Conference on Innovations for Community Services, pp. 221–232. Springer, Cham (2019)
14. She, W.E.I., Gu, Z.-H., Lyu, X.-K., Liu, Q.I., Tian, Z., Liu, W.: Homomorphic consortium blockchain for smart home system sensitive data privacy preserving. IEEE Access **7**, 62058–62070 (2019)

15. Kafle, Y.R., Mahmud, K., Morsalin, S., Town, G.E.: Towards an internet of energy. In: Proceedings of the nternational Conference on Power System Technology (POWERCON), Wollongong, pp. 1–6 (2016)
16. Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., Bertoncini, M.: Blockchain based decentralized management of demand response programs in smart energy grids. Sensors **18**(1), 162 (2018)
17. Lundqvist, T., de Blanche, A., Andersson, H.R.H.: Thing-to-thing electricity micro payments using blockchain technology. In: Proceeding of the Global Internet Things Summit (GIoTS), Geneva, pp. 1–6 (2017)
18. Pop, C., Cioara, T., Antal, M., Anghel, I., Salomie, I., Bertoncini, M.: Blockchain based decentralized management of demand response programs in smart energy grids. Sensors **18**(1), 162 (2018)
19. Shae, Z., Tsai, J.J.P.: On the design of a blockchain platform for clinical trial and precision medicine. In: Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, pp. 1972–1980 (2017)
20. Marsal-Llacuna, M.-L.: Future living framework: Is blockchain the next enabling network? Technol. Forecast. Soc. Change **128**, 226–234 (2018)
21. Sharma, P.K., Park, J.H.: Blockchain based hybrid network architecture for the smart city. Future Gener. Comput. Syst. **86**, 650–655 (2018)
22. Hang, L., Kim, D.-H.: Design and implementation of an integrated IoT blockchain platform for sensing data integrity. Sensors **19**(10), 2228 (2019)
23. Zhang, iY., Wen, J.: An IoT electric business model based on the protocol of Bitcoin. In: Proceedings of the 18th International Conference on Intelligence in Next Generation Networks, Paris, pp. 184–191 (2015)
24. Yuan, Y., Wang, F.-Y.: Towards blockchain-based intelligent transportation systems. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), pp. 2663–2668. IEEE, Piscataway (2016)
25. Wilson, D., Ateniese, G.: From pretty good to great: Enhancing PGP using Bitcoin and the blockchain. In: Proceedings of the International Conference on Network and System Security, New York, pp. 368–375 (2015)
26. Werbach, K.: Trust, but verify: Why the blockchain needs the law. Berkeley Tech. LJ **33**, 487 (2018)
27. Yang, M., Zhu, T., Liang, K., Zhou, W., Deng, R.H.: A blockchain-based location privacy-preserving crowdsensing system. Future Gener. Comput. Syst. **94**, 408–418 (2019)
28. Tanas, C., Delgado-Segura, S., Herrera-Joancomartí, J.: An integrated reward and reputation mechanism for MCS preserving users' privacy. In: Proceedings of the 10th International Workshop Data Privacy Management, Security Assurance, vol. 9481, pp. 83–99. Springer, New York (2016)
29. Korpela, K., Hallikas, J., Dahlberg, T.: Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
30. Kshetri, N.: Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun. Policy **41**(10), 1027–1038 (2017)
31. Strobel, V., Castelló Ferrer, E., Dorigo, M.: Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario. In: Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems (AAMAS) (2018)
32. Dorri, A., Kanhere, S.S., Jurdak, R.: Blockchain in internet of things: Challenges and solutions (2016). Preprint arXiv:1608.05187
33. Hernández-Rojas, D.L., Fernández-Caramés, T.M., Fraga-Lamas, P., Escudero, C.J.: Design and practical evaluation of a family of lightweight protocols for heterogeneous sensing through BLE beacons in IoT telemetry applications. Sensors **18**(1), 57 (2017)
34. Fraga-Lamas, P., et al.: Enabling automatic event detection for the pipe workshop of the shipyard 4.0. In: Proceedings of the 56th FITCE Congress, Madrid, pp. 20–27 (2017)

35. Maksymyuk, T., Gazda, J., Han, L., Jo, M.: Blockchain-based intelligent network management for 5G and beyond. In: 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), pp. 36–39. IEEE, Piscataway (2019)
36. Tian, F.: 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), pp. 1–6. IEEE, Piscataway (2016)
37. Vukolić, M.: The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. Available: http://www.vukolic.com/iNetSec_2015.pdf (2015). Accessed 10 Apr 2018

Chapter 5
Leveraging Blockchain Technology for Artificial Intelligence

Artificial intelligence (AI) and blockchain are among the most promising and widely deployed technologies in recent times. On the one hand, blockchain can enable interactions among clients without the presence of any trusted third party and provide access to a blockchain ledger that holds transactions, logs, and data in a decentralized, trusted, and secured manner. On the other hand, AI facilitates making intelligent decisions by observing the environment. This chapter presents an overview of integrating blockchain with AI technology, covering the importance, applications, challenges, and potential open research issues (Fig. 5.1).

5.1 Importance of Integrating Blockchain with AI

In Chaps. 1 and 2, we already discussed the fundamental details of blockchain technology. The area of artificial intelligence (AI) can be defined as the study of empowering intelligence to machines that could perceive their surroundings and take necessary actions accordingly [1]. Specifically, AI is the engineering and science for developing intelligent machines using computer programs that facilitates computers the sophistication to understand the environment and act intelligently [2, 3]. Few examples of AI applications are expert systems [4], decision-making AI [5], digital twins [6], hybrid learning models [7–9], and automated machine learning [10, 11]. The integration of blockchain with such applications can help us to develop decentralized AI applications with a secured and trusted platform. The machine learning algorithms perform better when the collected data are tamper-free, reliable, and secure. As in blockchain, the data on the distributed ledger is inserted into the block after being verified, signed cryptographically, and passed the consensus mechanism. If we design a smart contract to apply machine learning while making prediction, performing analytics, or making a decision, the outcome would have more reliability, integrity, and consistency than the conventional machine learning

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_5

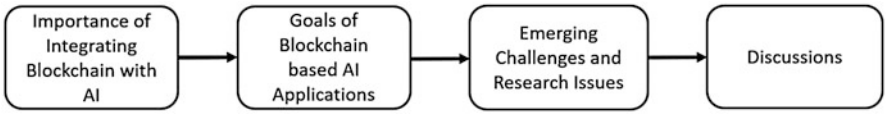

Fig. 5.1 Chapter overview

Table 5.1 Core features and relevant benefits of coupling blockchain with AI

Blockchain	AI	Benefits of blockchain + AI
Decentralized	Centralized	Improves security
Deterministic	Variable	Improves trust
Immutable	Probabilistic	Improves decision-making process
Integrity	Volatile	Decentralized decision-making
Attacks resistant	Discovers knowledge and makes decisions	High efficiency

approach. Particularly, the concept of integrating blockchain with AI technology could have significant improvements in data leakage or attack-prone areas such as medical, personal, military, baking, trading, and financial.

In Table 5.1, we present some remarkable features of coupling blockchain with AI that are summarized as follows.

5.1.1 Improved and Secured Decision Outcomes

All transactions stored in blockchain are digitally signed and work in a decentralized way. Each respective client keeps secret their private keys and shares distributed ledger. As the data within the blockchain ledger are tamper-resistant, it enables AI algorithms to construct an intelligent system with secure data that ensures more trustworthy and reliable decision outcomes.

5.1.2 Collaborative Decision and Decentralized Intelligence

In various AI systems, the agents may need to take distributed decisions and send them to a central coordinator. Furthermore, the coordinator undertakes a cumulative decision based on the response of the agents. However, in the conventional AI approach, the agents' feedback may be tampered, which may influence the overall decision-making process. The integration of blockchain can help prevent such issues as the distributed agent's feedback can be stored in a public ledger to tamper-proof.

5.1.3 Reliable and Trustworthy Intelligent Decisions

The AI-based systems cannot attract consumers if it becomes dysfunctional or fails to work properly due to security holes or data temperament that leads to lack of trust on that product. The integration of blockchain in such AI systems can increase public trust by guaranteeing that data is not tampered with as each transaction record is included into the ledger after validation. The dependency on a centralized third-party entity will be eliminated as decisions can be made in a completely decentralized way.

5.1.4 Higher Efficiency

Business organizations that involve multiple stakeholders are inefficient as they need to verify a transaction through multiparty authorization. The coupling of AI with blockchain technology can enable automatic and faster validation of transactions that are occupied by different stakeholders, and thus, it accelerates the efficiency of the whole process.

5.2 Goals of Blockchain-Based AI Applications

The decentralization of AI applications is challenging as the applications need to perform planning, searching, learning, optimization, and decision-making—all in a decentralized fashion. In this section, we discuss the way to achieve decentralized operations of AI applications.

5.2.1 Autonomous Computation

To construct a decentralized AI system, one of the key points is to ensure decentralized and local AI agents' computations. The agents are basically the entities responsible for sensing the environment, collecting data, and performing operations according to their state. Suppose we want to enable decentralized operations of those agents. In that case, we need to effectively handle those agents' heterogeneity in terms of data sources, systems configurations, application interfaces, data, storage, and processing systems [12]. The integration of blockchain ensures to preserve the interaction among multiple agents, sensitive data, systems, and application information that lead to fully decentralized AI-based autonomous systems.

5.2.2 Planning

Another important feature of AI applications is planning that is required to make strategies to perform collaboration with other applications, adjust in new environments, and solve complicated problems [13]. Particularly, planning is required to accelerate the efficiency and ensure the resilience of AI-based applications. The existing centralized planning of AI applications is time-consuming and relatively complex. Thus, blockchain-based decentralized planning is needed to bring simplicity, integrity, robustness, and efficiency. Besides, if the planning strategies are immutable, that could be effective specifically in mission critical systems.

5.2.3 Discovering New Knowledge

The conventional centralized AI systems and applications need to analyze large amounts of data for discovering knowledge or useful patterns. However, the centralized AI systems are difficult to manage while discovering personalized knowledge patterns and retrieving customized patterns for specific users. The fusion of blockchain in AI-based systems can generate personalized knowledge patterns through decentralized fashion and can facilitate by ensuring traceable and immutable knowledge transfer among multiple agents in AI systems [14].

5.2.4 Perceive Environment

The intelligent agents in centralized AI systems and applications are programmed to sense, collect, interpret, choose, and arrange data that incurs monolithic data collection [15]. There is a huge risk of data temperament while transferring collected data through the perception process. Applying decentralized perception strategies can enable tracing perception strategies of the agents, secure and immutable data storage and data transfer, and eliminate the risk of data temperament while transferring data or exchanging information [16].

5.2.5 Efficient Searching

The autonomous agents in AI applications and systems may need to search a large dataset that is prepared during operation within a large and sparse environment. That is why an efficient searching method is required to carry out the AI agents' smooth operations and decision-making process. In a centralized AI application and system, the stored data can be repeatedly reorganized or tampered due to the new input data

or security attacks. However, the integration of blockchain technology can help to store the collected data in sequential blocks securely, resisting any temperament, and can also assist in achieving optimal solutions of the searching mechanism by keeping previous successful search traces. Besides, efficient block searching process (e.g., [17]) can also be adapted to accelerate the process of decentralized AI.

5.2.6 Optimization of Decision-Making Process

One key point to develop an efficient AI system and application is to choose the best choice for AI agents among all the possible options. Selection of best possible choices can be achieved by selecting the best candidate, most effective data source, selecting the best traversal path during searching, and applying the most efficient data management and storage technique for the related environment. Leveraging decentralized optimization can help to accelerate system performance through the processing of distributed resources. It is even more useful when we need to simultaneously run multiple agents with their different optimization objectives across various AI applications and systems.

5.3 Emerging Challenges and Research Gaps

This section discusses the emerging challenges and research gaps of developing and implementing decentralized AI-based applications and systems that include privacy, security, blockchain interoperability, regulations, consensus protocols, governance, and trust issues.

5.3.1 Privacy

In a public blockchain, all collected information by the agents is stored in public ledgers accessible for all clients within the network. We can apply blockchain technology within an AI-based system for constructing a forecasting model or making intelligent decisions. However, the collected data could be sensitive, and keeping those private data into public, ledgers could open up the risk of privacy violations. Though adapting private blockchain can solve the issue of public accessibility of the sensitive data, that would limit the data availability and degrade the decision-making process's performance.

5.3.2 Security

The consensus mechanism of blockchain can suffer from security risks, e.g., 51% attack [18] even when we infuse blockchain with AI technology for making decentralized intelligent decisions. If the consensus protocols are compromised, then the decentralized systems can be turned into centralized as few miners would control the blockchain. A public blockchain (e.g., Bitcoin, Ethereum) is more prone to such security risks as anyone can access the blockchain ledgers and join the blockchain network. Private and permissioned blockchains are comparatively less prone to such attacks as the accessibility of such blockchain ledgers is limited, and consensus protocols are previously defined among the trusted parties. However, in a private blockchain, the execution outcomes can be influenced or changed through the unstable execution of the mining nodes (e.g., hyperledger) [12]. To handle such a problem, the latest blockchain platform ensures the execution of the mining nodes in a Trusted Execution Environments (TEEs) [19].

5.3.3 Scalability

Scalability is regarded as one of the major challenges of today's blockchain-based AI applications. While blockchain-based applications can perform only a few transactions per second, applications without blockchain (e.g. Twitter) can perform millions of transactions per second [20]. To accelerate the performance of blockchain, sidechains [21] are used that can enable transactions among various AI agents outside the main chain. More extensive research needs to be conducted to increase the number of transactions per second for blockchain-based AI applications.

5.3.4 Consensus Protocol Design for AI Applications

The currently trading blockchain systems are designed with blockchain protocols by considering blockchain networks and their middleware layers. However, the future blockchain protocols could be designed by considering AI applications' characteristics, e.g., data quality, optimization, data management, and search strategies.

5.3.5 Blockchain Regulations and Interoperability

There is no standard set of rules and regulations of blockchain, and in consequence, it becomes challenging to perform interoperability among multiple blockchain. It is

because different blockchains may hold different architecture, consensus protocols, governance, and policies. Therefore, ensuring secured transactions passing the consensus stage and maintaining different blockchains policies becomes challenging. Further research needs to be conducted to define a standard set of rules and consensus protocols for swift operations of blockchain interoperability.

5.3.6 Governance

The designing, planning, deployment, validation, and managing of a blockchain among multiple stakeholders and participants are interminable tasks. Selection of blockchain type, managing, and troubleshooting, preparing a smart contract, choosing trusted miners, integrating sidechains, off-chain activities, and maintaining standards and regulations—all decisions need to be made by the blockchain governance [22, 23]. Therefore, effective governance models are required to develop for managing blockchain efficiently.

5.4 Discussion

In this chapter, we discuss the importance of infusing blockchain with AI applications and systems. We describe the goals of blockchain-based AI applications that reflect the essential points that need to ensure while enabling decentralized intelligence. Furthermore, we present the existing core challenges and research issues while deploying blockchain technology for AI. This reflects the necessities and directions of addressing challenges related to privacy, security, scalability, consensus protocols, and governance in future research.

References

1. Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach. Pearson, London (2002)
2. Nilsson, N.J.: Principles of Artificial Intelligence. Morgan Kaufmann, Burlington (2014)
3. McCarthy, J.: What Is Artificial Intelligence. Computer Science Department, Stanford University, vol. 2 (2007)
4. Liebowitz, J. (Ed.): The Handbook of Applied Expert Systems. CRC Press, Boca Raton (2019)
5. Samek, W., Wiegand, T., Müller, K.-R.: Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models (2017). Available: https://arxiv.org/abs/1708.08296
6. El Saddik, A.: Digital twins: The convergence of multimedia technologies. IEEE Multimed. **25**(2), 87–92 (2018)
7. Alcalá, R., Alcalá-Fdez, J., Casillas, J., Cordón, O., Herrera, F.: Hybrid learning models to get the interpretability—accuracy trade-off in fuzzy modeling. Soft Comput. **10**(9), 717–734 (2006)

8. Huang, Y., Kechadi, T.: An effective hybrid learning system for telecommunication churn prediction. Expert Syst. Appl. **40**(14), 5635–5647 (2013)
9. Zameer, A., Khan, A., Javed, S.G.: Machine Learning based short term wind power prediction using a hybrid learning model. Comput. Electr. Eng. **45**, 122–133 (2015)
10. Feurer, M., Eggensperger, K., Falkner, S., Lindauer, M., Hutter, F.: Practical automated machine learning for the AutoML challenge 2018. In: International Workshop on Automatic Machine Learning at ICML, pp. 1–12 (2018)
11. Kraft, A.W., Sanat Kumar Dhua, A., Ryan Gray, D., Lin, X., Yu, L.O.U., Ramesh, S., Jon Taylor, C., Creighton Mott, D.: Automated highlighting of identified text. U.S. Patent 9,582,913 (2017)
12. Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: review and open research challenges. IEEE Access **7**, 10127–10149 (2019)
13. Laborie, P.: Algorithms for propagating resource constraints in AI planning and scheduling: existing approaches and new results. Artif. Intell. **143**(2), 151–188 (2003)
14. Ekramifard, A., Amintoosi, H., Hosseini Seno, A., Dehghantanha, A., Parizi, R.M.: A systematic literature review of integration of blockchain and artificial intelligence. In: Blockchain Cybersecurity, Trust and Privacy, pp. 147–160. Springer, Cham (2020)
15. Lu, H., Li, Y., Chen, M., Kim, H., Serikawa, S.: Brain intelligence: go beyond artificial intelligence. Mobile Netw. Appl. **23**(2), 368–375 (2018)
16. Zheng, Z., Dai, H.-N., Wu, J.: Blockchain intelligence: When blockchain meets artificial intelligence (2019). Preprint arXiv:1912.06485
17. Morishima, S., Matsutani, H.: Accelerating blockchain search of full nodes using GPUs. In: 2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), pp. 244–248. IEEE, Piscataway (2018)
18. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. 107, 841–853 (2017). https://doi.org/10.1016/j.future.2017.08.020
19. Brandenburger, M., Cachin, C., Kapitza, R., Sorniotti, A.: Blockchain and trusted computing: Problems, pitfalls, and a solution for hyperledger fabric (2018). Available: https://arxiv.org/abs/1805.08541
20. Zhou, Q., Huang, H., Zheng, Z., Bian, J.: Solutions to scalability of blockchain: a survey. IEEE Access **8**, 16440–16455 (2020)
21. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains (2014). http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 72
22. Reijers, W., O'Brolcháin, F., Haynes, P.: Governance in blockchain technologies & social contract theories. Ledger **1**, 134–151 (2016)
23. Beck, R., Müller-Bloch, C., Leslie King, J.: Governance in the blockchain economy: a framework and research agenda. J., Asso. Inf. Syst. **19**(10) 1 (2018)

Chapter 6
Coupling Blockchain with Emerging Real-Life Applications

This chapter discusses some real-life blockchain-based applications and describes the applicability and necessity of integrating blockchain with the existing centralized systems. Particularly, we describe some widely popular domains where blockchain can be applied, i.e., healthcare, energy, finance, agriculture, smart city, smart manufacturing, e-voting, and personal identity management. To clearly understand the applications, we present visual representations of deploying blockchain's conceptual understanding within those real-life applications. Prior works [1–6] highlight the potential areas or domains for blockchain technology. This chapter presents in detail how blockchain can be blended with those areas to provide a secure service.

6.1 Blockchain in Healthcare

Blockchain technology is considered to have a huge impact on healthcare applications, because healthcare data are sensitive and the leakage or modifications of any such data due to cyber-attacks could have a vital negative impact on hospital authorities and patients. The digitalization of healthcare service opens up the opportunity to track a patient's data and provide assistance by remotely monitoring the health conditions. For example, a senior citizen who is unable to go to a hospital due to health issues, resource shortage, or contagious virus (e.g., Severe Acute Respiratory Syndrome (SARS), Wuhan Novel Coronavirus) can be monitored (e.g., blood pressure, heartbeat, oxygen level) through wearable devices that continuously pass data to the hospital server. Such advancement creates security and privacy concerns as the patient data is directly shared with a third party, and it imposes the risk of altering any sensitive information. However, if the hospital adapts the blockchain technology, any transaction related to patient records (e.g., health data, drug information) would be protected and secured. There would be

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_6

no possibility of data modification that may otherwise result in drug counterfeit, personal information leak, etc. Besides, blockchain can be applied for reliable storage of drug prescriptions, secure access control, supply chain management, and sharing and accessing of patient information. Different healthcare sectors can also benefit from blockchains such as medical billing, clinical trials, exchanging medical records, agreements with other hospitals or organizations, and anti-counterfeiting trade agreements. Due to the robustness of blockchain technology and secure access control over patients' health records, the security and reliability of patients' data are enhanced, particularly while exchanging medical records with different healthcare systems [7]. In Fig. 6.1, we presented some healthcare domains that can adapt blockchain for secure operations.

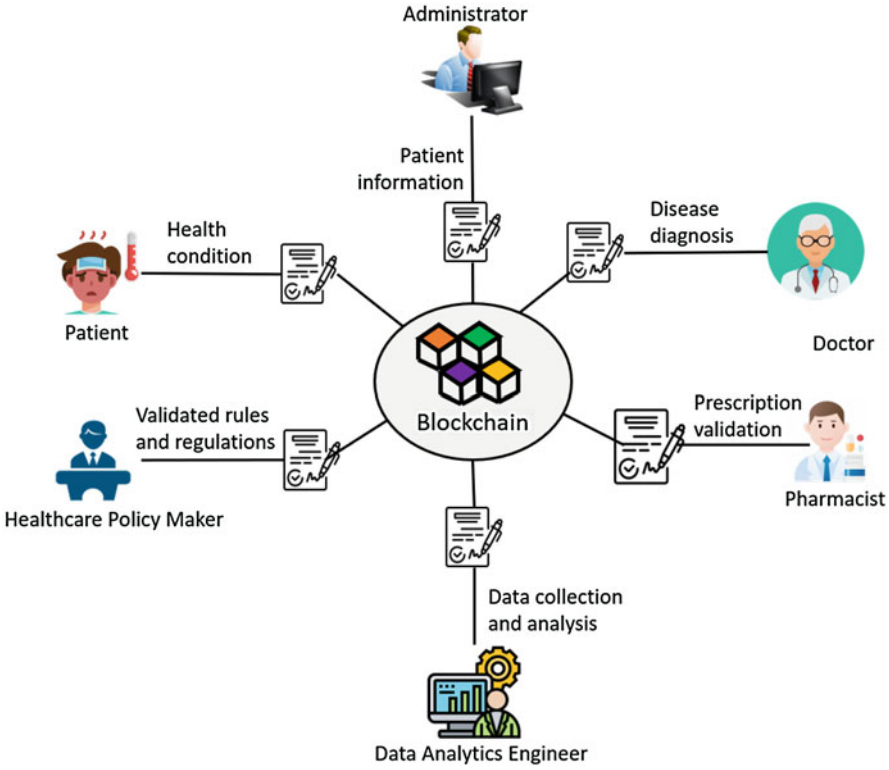

Fig. 6.1 Blockchain applications in healthcare

6.2 Energy Market Trading

It is essential to ensure fair, transparent, and trusted energy trading between two parties residing in a distributed environment in energy market trading. The power of blockchain technology provides secure P2P trading between the blockchain users of the energy network [8, 9]. For example, the energy market trading concept is applicable while designing a resilient system for smart grids. The energy status information of the energy resources can be obtained through IoT and can be stored in an immutable and secure distributed ledger. The authors in [10, 11] discussed peer-to-peer energy resource exchange for distributed grids that enables examining the matching or similarities between generation and load at a distribution level. The optimal matching between loads and generators reduces the relative cost of energy, makes effective utilization of unused power, and ensures lower transmission line congestion. Besides, blockchain can be effective in the maintenance and service purposes of electric components and machines. For instance, we can consider electric vehicles (EVs) that possess the scarce changing infrastructure and encounter complexity while deploying them [12]. Blockchain provides secure services and simplifies the charging process that makes the maintenance of EVs convenient and cheaper. The charging and discharging operations of EVs can be executed by analyzing electricity and smart contracts' requirements and can be worked as batteries to handle energy allocation. In the case of energy market trading between multiple grid agents, a smart contract or an agreement (details on the smart contract are given in Chap. 2) can be created, and we can spread that over the network. None of the parties can refuse the agreement due to traceability, and the identity of the transacted parties remains anonymous. Besides, the guarantee of immutable information about distributed energy resources can help us to discover reliable knowledge and perform efficient, intelligent decisions. In Fig. 6.2, we presented a high-level overview of a blockchain-based energy market trading scenario.

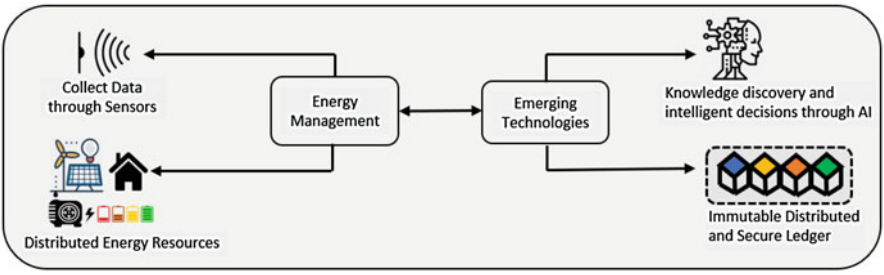

Fig. 6.2 Applying blockchain in energy market trading

6.3 Banking and Finance

The fragmented banking systems can also benefit from blockchain technology. The blockchain revolution can solve the issue related to trust, transparency, and confidentiality. Due to the intermediary regulatory process and clearance of operational trade, the customers need to wait for a long processing time to process their transactions [13]. Such delays cause trouble for the traders, brokers, regulators, and all other involved parties/stakeholders. Blockchain can resolve this issue by establishing authentication, confidentiality, non-repudiation through asymmetric cryptography and ensuring the clients' security and privacy through decentralization. Blockchain eliminates the intermediary processes and monotonous paperwork while dealing with the financial exchange and legal transfer ownership. Figure 6.3 represents the applicability of blockchain technology in the banking and finance sector.

6.4 Agriculture and Food Supply Chain

Blockchain technology has brought a revolutionary change in the notion of trust by demonstrating its improved efficiencies toward sustainable agricultural development. When the blockchain-based agricultural infrastructure is constructed with the immutable distributed record management strategy, the integrity of the baseline agricultural data is safeguarded for the participants involved in the transparent data management [14]. The agriculture sectors include farmland monitoring, secure transactions, quality assurance, trustworthy logistics support, reliable decision-making, and predictive analysis, and analyzing a product's market status. The

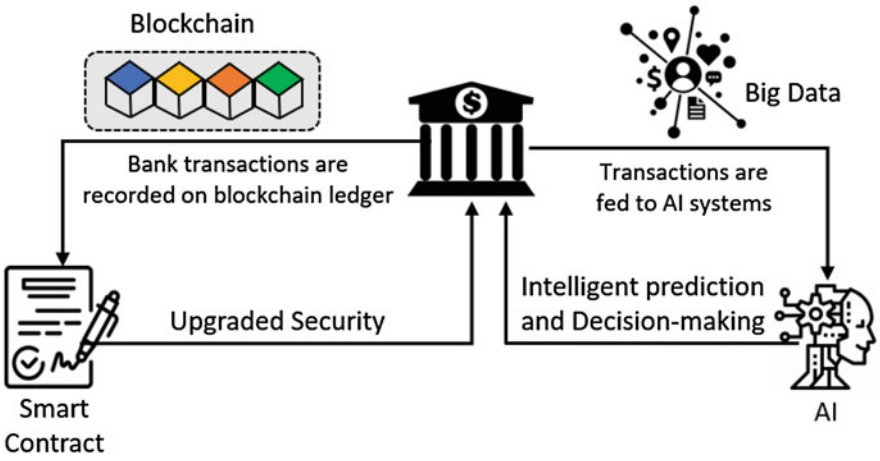

Fig. 6.3 Applicability of blockchain in banking and finance sectors

evaluation of IoT technology enables tracking agricultural products and monitoring farmland conditions, and blockchain technology protects those data by encapsulating them within secure blockchain blocks. Any predictive analysis can be performed from those extracted data, and necessary steps can be taken according to the forecasting results [15]. Besides, while dealing with customers about products, a smart contract can be signed between both parties that ensure secure and reliable asset transfer. Further, in a food supply chain, a product may consist of multiple parts supplied by different manufacturers. However, some low-quality or forged product may be included in the supply chain. It is costly to apply anti-fraud systems for every single part of a product throughout the process life-time in such a situation. The integration of blockchain and IoT concept can be used to mitigate such a high cost and identify any low-quality product. Each product can be attached with a unique ID, timestamp, product-quality status, and other necessary information. The identification of each part is saved into the blockchain, which is immutable and traceable. Later on, even any changes within the item reveal the tampered product, and the supplier can easily trace and replace that. In this way, the integration of blockchain with IoT helps to fasten production speed, reduce cost, and enable flexible operations in supply chain management. In Fig. 6.4, we illustrated the blockchain applicability within different domains of smart farming.

6.5 Smart City

A smart city's infrastructure consists of traffic management, surveillance of roads and highways, optimal road light control, monitoring environment, smart waste management, and parking, etc. All these applications of a smart city are dependent on the idea of the Internet of Things (IoT). The improved infrastructure and widespread availability of internet facility enable deploying smart city in an effective fashion [16–18]. The applications of smart cities are mostly dependent on the collected and observed data by IoT devices that are integrated with the system

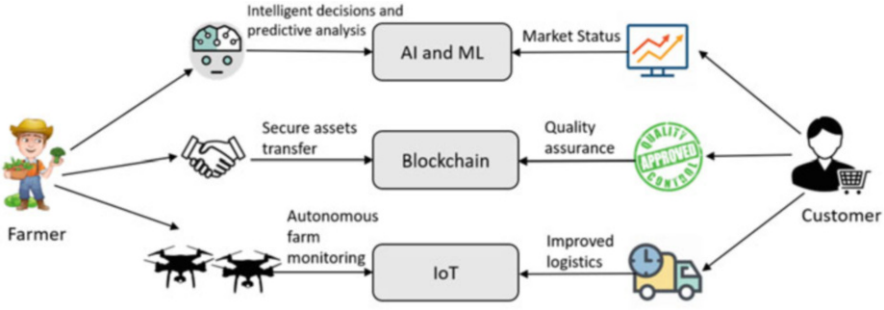

Fig. 6.4 Integrating blockchain to ensure secure and smart agriculture

environment. Any data extracted by the sensors or video data captured by the camera can be further used for analysis, decision-making, constructing a prediction model, or identifying useful information. However, due to the heterogeneous nature and resource-constrained issues, a smart city is prone to vulnerable attacks [19, 20]. To avoid such attacks, storing the collected and observed data in a secure and trustless platform is indispensable. In Fig. 6.5, we presented different blockchain applications considering smart city infrastructure. The smart city applications include smart traffic management system by monitoring vehicle activities, and traffic flows by capturing and analyzing video data. Smart security includes personal property, organizations, or roadside surveillance, while smart road light control can be operated by determining vehicles' presence. A smart environment means capturing the weather and environmental information to understand the purity of nature, and a smart waste management system refers to the waste bin status monitoring without any human involvement. Finally, smart parking helps to know about parking information of a particular area (e.g., free parking location). All these applications pass sensitive information of the users and their surroundings, and any leakage or slight modifications of the collected data can hamper any related operations or decision-making process. However, if those collected data can be handled and managed through blockchain technology, then it can accelerate the decision-making process due to its fast data validation process [21].

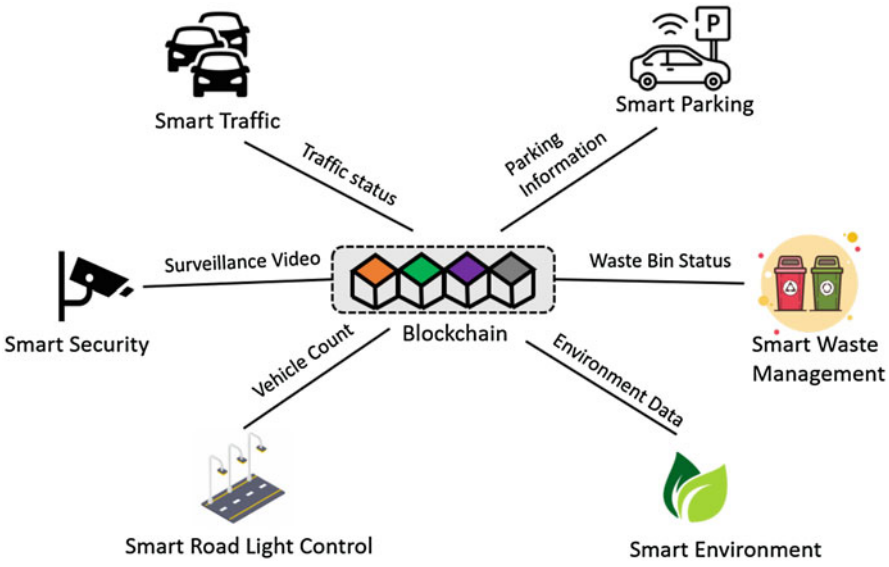

Fig. 6.5 Application of blockchain in smart city infrastructure

6.6 Smart Manufacturing

The manufacturing industries are experiencing an upgrade from automated to smart manufacturing. The analysis of manufacturing data plays a vital role in this regard. A vast amount of data is generated from the overall product life cycle, e.g., requirement gathering, product designing, supply information of raw material, production, distribution, maintenance, after-sales service [22–24]. An overview of different applications in smart manufacturing is illustrated in Fig. 6.6. The blockchain collects product information via a shared and secure record of the exchange. A product may be possessed by various actors, e.g., manufacturers, distributors, retailers, certifiers, operation management, registers, waste management, and finally, reach the customers. Each product can be attached with a tag in the form of RFID, barcode, or QR code. The tag can act as a cryptographic identifier and establish a link between the physical product and its virtual naming on the blockchain network. Each actor provides their relevant product information within the blockchain, and the information remains safe and secure. The actors can observe the product details according to their accessibility. Sometimes, a department may require the generated data from another department. We need to ensure immutability while exchanging that information among various departments or with another industry.

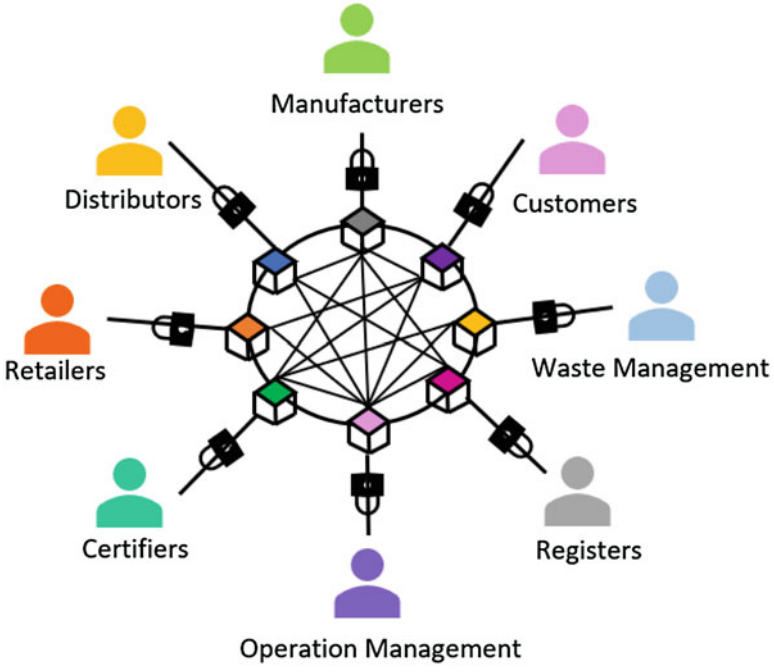

Fig. 6.6 Blockchain-based smart manufacturing process

Several blockchains can be constructed for different sections, and blockchain interoperability can be incorporated to obtain secure information exchange.

6.7 Voting

Another useful application of blockchain is constructing a voting platform. The conventional voting systems can be improved by leveraging blockchain. We need a mechanism that guarantees a vote to be counted without skipping or tampering. Blockchain can solve the matter by storing every vote in immutable and distributed ledgers [25–28]. In Fig. 6.7, we presented a blockchain-based e-voting scheme. Initially, each voter needs to provide credentials, and the respective authority examines the credentials. Further, the authenticated voter provides a signed vote in a smart contract that resides within a blockchain. The blockchain verifies the vote and generates a transaction id for that voter that is written in the smart contract. Any modifications of the vote generate a different transaction id, and hence, the block hash will be changed. As a result, the tampered block will not be a part of the chain anymore. Therefore, there is no chance of voting manipulation, and the voters are guaranteed that their vote would be counted.

6.8 Personal Identity Management

In today's world, personal identity is verified by matching an identity card (e.g., passport, driving license) of a person with the data stored on the server. However, it is possible to forge those private data, and any slight modification of data can bring a lot of trouble for that user. In such applications, blockchain can be an effective mechanism to secure the online identities of the users. Blockchain can allow a user

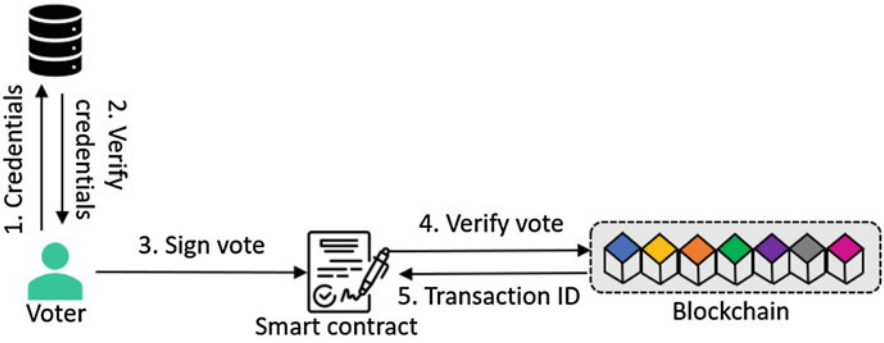

Fig. 6.7 Blockchain-based smart manufacturing process

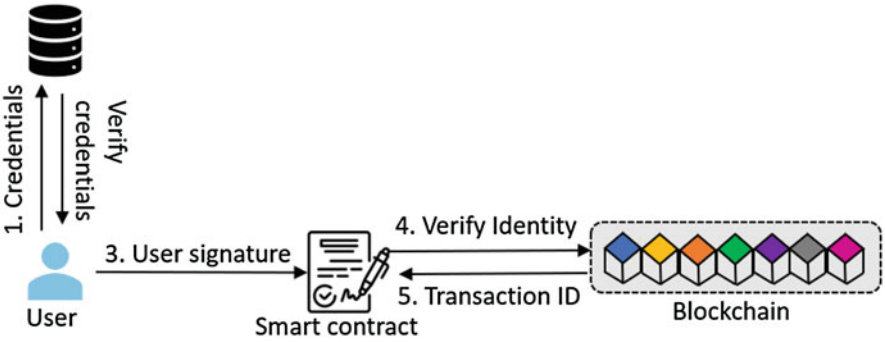

Fig. 6.8 Blockchain-based personal identity management

to create an encrypted identity without revealing its sensitive information and also can trace or identify any fraudulent activities of the systems [29]. A digital ID can be generated after adapting the blockchain principle, and any sensitive activities (e.g., payment, appointment) can be accessed and verified. It eliminates the risk of changing any user information, as any change would alter the block hash that results in isolation of the forged block from the main chain. In Fig. 6.8, we presented how a user identity can be signed, verified, and stored within a blockchain.

6.9 Discussion

In this chapter, we discuss various real-life blockchain applications and explain how the integration of blockchain technology has brought revolutionary changes, particularly in ensuring the security of those substantially popular applications. Throughout this chapter, we present high-level visual representations of the working mechanisms of different blockchain application domains with proper explanations that help the reader perceive a clear conception about the working process and the necessity of coupling blockchain technology emerging real-life applications.

References

1. Guo, Y., Liang, C.: Blockchain application and outlook in the banking industry. Financial Innov. **2**(1), 24 (2016)
2. Monrat, A.A., Schelén, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
3. Tse, D., Zhang, B., Yang, Y., Cheng, C., Mu, H.: Blockchain application in food supply information security. In: 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 1357–1361. IEEE, Piscataway (2017)

4. Dai, F., Shi, Y., Meng, N., Wei, L., Ye, Z.: From bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In: 2017 4th International Conference on Systems and Informatics (ICSAI), pp. 975–979. IEEE, Piscataway (2017)
5. Luo, X., Wang, Z., Cai, W., Li, X., Leung, V.C.M.: Application and evaluation of payment channel in hybrid decentralized Ethereum token exchange. Blockchain: Res. Appl. **1**(1–2), 100001 (2020)
6. Mougayar, W.: The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley, New York (2016)
7. Mettler, M.: Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th International Conference on e-health Networking, Applications and Services (Healthcom), pp. 1–3. IEEE, Piscataway (2016)
8. Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., Peacock, A.: Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renew. Sust. Energ. Rev. **100**, 143–174 (2019)
9. Amini, M.H.: Decentralized operation of interdependent power and energy networks: blockchain and security. In: Blockchain-based Smart Grids, pp. 61–73. Academic Press (2020)
10. Reihani, E., Siano, P., Genova, M.: A new method for peer-to-peer energy exchange in distribution grids. Energies **13**(4), 799 (2020)
11. Siano, P., G.D. Marco, A. Rolán, V. Loia: A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Syst. J. **13**(3), 3454–3466 (2019)
12. Chen, W., Xu, Z., Shi, S., Zhao, Y., Zhao, J.: A survey of blockchain applications in different domains. In: Proceedings of the 2018 International Conference on Blockchain Technology and Application, pp. 17–21 (2018)
13. Treleaven, P., Brown, R.G., Yang, D.: Blockchain technology in finance. Computer **50**(9), 14–17 (2017)
14. Apte, S., Petrovsky, N.: Will blockchain technology revolutionize excipient supply chain management? J. Excip. Food Chem. **7**(3), 910 (2016)
15. Bermeo-Almeida, O., Cardenas-Rodriguez, M., Samaniego-Cobo, T., Ferruzola-Gómez, E., Cabezas-Cabezas, R., Bazán-Vera, W.: Blockchain in agriculture: A systematic literature review. In: International Conference on Technologies and Innovation, pp. 44–56. Springer, Cham (2018)
16. Xie, J., Tang, H., Huang, T., Richard Yu, F., Xie, R., Liu, J., Liu, Y.: A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun. Surv. Tutor. **21**(3), 2794–2830 (2019)
17. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1392–1393. IEEE, Piscataway (2016)
18. Sharma, P.K., Moon, S.Y., Park, J.H.: Block-VN: A distributed Blockchain based vehicular network architecture in smart city. J. Inf. Proc. Syst. **13**(1), 184–195 (2017)
19. Biswas, K., Muthukkumarasamy, V.: Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1392–1393. IEEE, Piscataway (2016)
20. Liang, X., Shetty, S., Tosh, D.: Exploring the attack surfaces in blockchain enabled smart cities. In: 2018 IEEE International Smart Cities Conference (ISC2), pp. 1–8. IEEE, Piscataway (2018)
21. Rivera, R., Robledo, J.G., Larios, V.M., Avalos, J.M.: How digital identity on blockchain can contribute in a smart city environment. In: 2017 International Smart Cities Conference (ISC2), pp. 1–4. IEEE, Piscataway (2017)
22. Zhang, Y., Xu, X., Liu, A., Lu, Q., Xu, L., Tao, F.: Blockchain-based trust mechanism for IoT-based smart manufacturing system. IEEE Trans. Comput. Soc. Syst. **6**(6), 1386–1394 (2019)

23. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **5**(9), 1–10 (2016)
24. Li, Z., Barenji, V., Huang, G.Q.: Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. Robot. Comput. Integr. Manuf. **54**, 133–144 (2018)
25. Kshetri, N., Voas, J.: Blockchain-enabled e-voting. IEEE Softw. **35**(4), 95–99 (2018)
26. Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M., Hjálmtýsson, G.: Blockchain-based e-voting system. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983–986. IEEE, Piscataway (2018)
27. Ayed, A.B.: A conceptual secure blockchain-based electronic voting system. Int. J. Netw. Security Appl. **9**(3), 01–09 (2017)
28. Hsiao, J.-H., Tso, R., Chen, C.-M., Wu, M.-E.: Decentralized E-voting systems based on the blockchain technology. In: Advances in Computer Science and Ubiquitous Computing, pp. 305–309. Springer, Singapore (2017)
29. Devecchi, C., Hadawi, A., Turner, S., Armellini, A., Brooks, I., Mellish, B., Petford, N., Ta'eed, O.: Blockchain Educational Passport: Decentralised Learning Ledger (DLL). Seratio Blockchain White Paper 5 (2017)

Index

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1