Blockchain Technology-Comprehensive Analysis, Applications, and Emerging Challenges

Jianqi Mu

Blockchain Engineering, Chengdu University of Information Technology, Chengdu, 610225, China
2021131082@stu.cuit.edu.cn

Abstract. With the maturation and widespread adoption of technologies such as peer-to-peer networks (P2P), asymmetric encryption, and distributed storage, blockchain technology has surged to prominence, capturing the interest of scholars across diverse disciplines. This paper provides a historical overview of blockchain's development, analyzing and comparing its evolving characteristics through different stages to illustrate its progressive integration into society. Additionally, by classifying blockchain types and detailing its layered architecture, the paper offers a comprehensive analysis of blockchain technology. Furthermore, this article highlights the primary contemporary applications of blockchain across various sectors and discusses the challenges it currently faces. These include scalability, energy consumption, security vulnerabilities, and regulatory uncertainty. Through an exploration of these challenges, the paper identifies promising avenues for future research and development in blockchain technology. This includes enhancing its scalability, improving security measures, and fostering a clearer regulatory framework, all of which are crucial for harnessing blockchain's full potential in revolutionizing data management and transaction processes across global industries.

Keywords: Blockchain evolution, blockchain architecture, technology,

1 Introduction

Blockchain technology, an innovative paradigm in decentralized systems, leverages a constellation of foundational technologies including distributed consensus methods, digital signatures, and cryptographic hashes [1]. The term "blockchain" derives from its intrinsic data structure, comprising interconnected blocks and chains, a concept in computer science predating its current prominence. Stuart Haber and colleagues initially proposed digitally timestamping electronic documents in 1991 to protect against tampering, though this idea gained little attention until the advent of Bitcoin [2]. Created by Satoshi Nakamoto, Bitcoin represents the pioneering application of the Blockchain 1.0 era, enabling direct online payments between parties without financial intermediaries, thereby catalyzing interest in both cryptocurrencies and blockchain technology [3]. Subsequent developments by Vitalik Buterin with Ethereum introduced

© The Author(s) 2024
Y. Wang (ed.), *Proceedings of the 2024 2nd International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2024)*, Advances in Computer Science Research 115,
https://doi.org/10.2991/978-94-6463-540-9_27

smart contracts through the programming language Solidity, enhancing blockchain scalability and performance, and marking the beginning of the Blockchain 2.0 era [4]. Ethereum's innovation paved the way for the third phase of blockchain development, epitomized by Hyperledger, an open-source project initiated by the Linux Foundation to foster the application of blockchain technology beyond cryptocurrencies [5]. This broadened blockchain's application scope from finance to other sectors, enhancing its utility in areas such as supply chain management and information verification.

Compared to traditional internet technologies, blockchain's core characteristics, such as decentralization and auditability, have facilitated its adoption across various domains. After Bitcoin, the landscape of blockchain applications has expanded significantly, taking various forms and adapting to diverse contexts. Blockchains are categorized based on access permissions into public, consortium, and private types, each differing in their degree of decentralization [6]. Despite its integration of multiple technological advantages, blockchain faces significant challenges, such as Bitcoin's limitation of processing only seven transactions per second, a stark contrast to modern transactional needs [7]. This article examines the evolutionary path and fundamental principles of blockchain technology, offers an in-depth analysis of its architecture, and explores its burgeoning applications. Furthermore, it highlights the challenges confronting blockchain, outlining future developmental trends and its potential impacts across different sectors.

2 Relevant Theories

2.1 Development and Definition of Blockchain

Blockchain History. Blockchain technology is an innovative digital currency solution designed to minimize the risk of theft, carry-on difficulties, ownership determination issues, and assets being controlled by centralized authorities. While the first large-scale successful use of blockchain is Bitcoin in 2008, the concept of decentralized cryptocurrencies and applications had been mentioned since 1980s [8, 9]. As early as 1983, David Chaum proposed a revolutionary digital currency encryption scheme, which is about a blind signature scheme through e-Cash technology [10]. In 1997, British computer scientist Adam Back published an email in CryptoPunk titled "A Partial Hash Collision Based Postage Payments" [11]. He came up with a scheme to eliminate spam using hash calculations, namely proof of work (PoS). In 1998, the Chinese cryptographer Wei Dai proposed the technical idea of B-money, supposing that B-money is an electronic cash system that combines the PoS consensus mechanism and the distributed ledger. The first attempt to present the concept of producing money using decentralized consensus and computational problem solving was Wei Dai's b-money, although the proposal lacked sufficient details on how to put decentralized consensus into practice [12]. After that, a paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” supposed the revolutionary concept of cryptocurrency in 2008, author Nakamoto also coined the term “blockchain” to describe the innovative data structure used for recording transaction ledgers. The term blockchain technology

is generally believed to have originated from the open-source project Bitcoin and the birth of Bitcoin marks the official application of blockchain technology to the practical application of society.

At present, the development process of blockchain is divided into three main stages, namely the blockchain 1.0 stage with programmable digital cryptocurrency as the main feature, the blockchain 2.0 stage mainly implemented as a programmable financial system and blockchain 3.0 extends this innovative technology to a programmable society [13]. The following is an overview of each of the three phases of blockchain:

Blockchain 1.0. The salient feature of the blockchain 1.0 phase is that it has succeeded in driving the widespread adoption of cryptocurrencies, which is seen as the key feature of this phase. All currencies with fungible functions, including Bitcoin, are core products that belong to this stage. The first phase of blockchain uses proof of work (PoW) to make peers reach consensus. For example, in the Bitcoin system, participants compete for computing power to preemptively calculate the hash value less than or equal to the target to compete for block rights and obtain token rewards, and the duration of this process will be dynamically controlled to about 10 minutes. Therefore, the performance of the application in the blockchain 1.0 stage is generally very low, and the core language used is a simple scripting language, which is not Turing-complete, so the scalability is also very low.

Blockchain 2.0. Although the blockchain 1.0 phase has successfully promoted the widespread adoption of cryptocurrencies based on blockchain systems, it also faces some problems. For example, the competition for computing power in the PoW consensus mechanism has led to a large amount of waste of computing power and energy, as well as low efficiency. In addition, its simple stack scripting language cannot meet the needs of more complex application scenarios. Russian Vitalik Buterin published the Ethereum whitepaper in 2013, proposing to improve the performance and scalability of the blockchain system by introducing smart contracts [14]. The emergence of Ethereum has been recognized by a large number of developers and users, making it the most representative product of the blockchain 2.0 stage. Compared with blockchain 1.0, blockchain 2.0 takes smart contracts as its core function, and at the same time adds new options to reach consensus. The most famous one is proof-of-stake (PoS), which greatly improves the performance by reducing the block generation time. Smart contracts also use special languages such as Solidity to achieve more complex logical operations.

Blockchain 3.0. Compared with Blockchain 1.0 and Blockchain 2.0, the Blockchain 3.0 stage has a very significant improvement in scalability, adaptability and sustainability. The blockchain 3.0 phase marks the beginning of the real penetration of blockchain technology into all application fields of society. At this stage, Hyperledger is a representative achievement that demonstrates the wide range of application possibilities of blockchain technology. Hyperledger is a project built by the Linux Foundation, it aims to create an open-source distributed ledger framework and code

collaboration through a cross-platform and industry approach, promoting the cross-industry application of blockchain technology [15]. The core function of blockchain 3.0 is a digital value exchange application platform, and more efficient consensus algorithms such as Raft, Practical Byzantine Fault Tolerance (PBFT) have been introduced. Blockchain applications at this stage also support high-level programming languages such as JavaScript and Go.

The following Table 1 compares the characteristics of blockchains at different stages:

Table 1. Comparison of Blockchains at Different Stages.

Stage	Core features	Conseusus mechanism	Performance	Prograннmg language
Blockchain 1.0	Cryptocumencies	PoW	LOw	Simple scripting 1anguage
Blockchain 2.0	Smart contracts	PoWPoS	Average	Specialized language
Blockchain 3.0	Digital value trading platform	Raft/ PBFT and others	High	High-level programming 1anguages

Blockchain overview. Blockchain integrates a variety of modern technologies, such as asymmetric encryption, P2P networks, and hashing algorithms. At present, the industry has not yet formed a unified definition of blockchain. In a narrow sense, blockchain is a chain of blocks that stores data and a chain of data structures that link those blocks, which allows the data in different blocks to be correlated with each other. Broadly speaking, blockchain is a distributed database applying encrypted copied data on every peer to protect information. As a revolutionary technology, blockchain has the following important characteristics:

Decentralization: On contrast to a centralized system, any two peers can deal with each other in the blockchain system without requiring central agency authentication. Based on this feature, there's no need to spend a lot of money and manpower to maintain a central server like traditional database.

Autonomy: Generally, all business dealings are founded on trust, which ensures that each party can rely on the other to keep their promises. Blockchain achieves trust and autonomy among nodes through some certain kinds of the consensus mechanisms, with the aim of electing the correct decision through voting.

Auditability: Within a blockchain network, every transaction is documented by a digital distributed ledger and verified by a digital timestamp. This means that it is possible to find and audit information such as historical transactions by accessing any node in the blockchain system.

Automatic: By writing smart contracts, the storage of on-chain data and the automatic execution of transactions can be realized. Each node in the blockchain system is able to automatically authenticate data and transactions according to a given consensus mechanism.

2.2 The Blockchain System

Types of Blockchain. According to the openness of the blockchain system to participants, the blockchain can be divided into three types: public blockchain, private blockchain and consortium blockchain. The key distinction between these three types of blockchains is the consortium is somewhat centralized, the private blockchain is under the jurisdiction of a centralized body, and the public blockchain is completely decentralized. Here's an overview of each of the three different blockchains:

Public blockchain. The public blockchain is open to all participants and data is completely open and transparent. Participants can view and transmit transactions, take part in consensus processes, and keep up the shared ledger, which means this kind of blockchain is truly decentralized. Public blockchain typically uses Byzantine fault-tolerant algorithms such as PoW. Although highly decentralized, due to the need to reach a wide range of consensus, public blockchain's performance is low and limited by the single-point performance of nodes and network bandwidth, thus the scalability is poor.

Private blockchain. Compared to public blockchain, only authenticated entities can join private blockchain. Due to the fact that the nodes that join need to meet certain conditions and are strictly restricted by a single regulatory organization, the performance and scalability of the private blockchain are the highest, but the degree of decentralization is the lowest.

Consortium blockchain. The consortium chain is similar to a private chain, but is controlled by multiple organizations. This kind of blockchain and private blockchain generally use more efficient consensus algorithms like Practical Byzantine Fault Tolerance (PBFT), Raft, etc. Due to the larger consensus range involved in the consortium blockchain, its performance, scalability and decentralization are between private and public blockchains. The comparison of these three types blockchain is shown in the Table 2 below:

Table 2. Comparison of Different Kinds of Blockchain.

Characteristic	Public blockchain	Consortiu m blockchain	Private blockchain
Consensus Mechanism	Proof of work (Pow), Proof of stake (PoS)...	Practical Byzantine Fault Tolerance (PBFT) Raft ...	
Decentralization	High	Medium	LOW
Performance	Low	Relatively High	High
Scalability	Low	Relatively High	High

Blockchain Architecture. From the logical architecture of the blockchain system, six different layers make up the whole system based on each layer's ability and framework. Here's an overview and resolution of each layer:

Data layer. The data layer mainly contains blocks and their chain structure, accounts, transactions, ledgers and addresses.

The block implementation may differ depending on the platform or application, and it contains version, the hash of the previous block, the Merkle tree Root aggregates

included transactions' hashes, and the nonce used for consensus is combined with the timestamp for traceability. The Merkle tree, which is used to store and verify the transactions, is stored in the body of block. The data structure of the block is shown in the following Fig. 1:

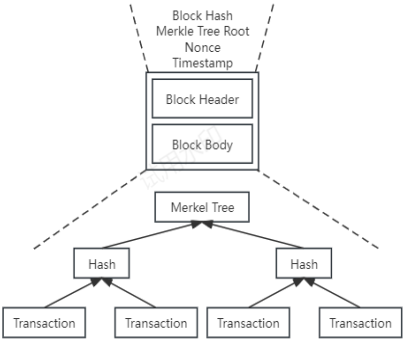

Fig. 1. Data Structure of Block .

The chain structure is the latest main chain formed by the newly generated blockchain linked with the previous blockchain by miners who have obtained the right to keep accounts. In blockchain 1.0, addresses were used and the account model was really introduced in blockchain 2.0.

Network layer. The blockchain network layer is responsible for the exchange and communication of information between nodes. This layer mainly contains the peer-to-peer(P2P) network model, propagation and verification mechanisms. The verification and propagation mechanisms vary according to different blockchain systems.

The P2P network uses a distributed network design to allow users to share resources. As a network model that does not have central characteristics, the P2P network provides good system robustness and security for blockchain system. The blockchain 1.0 uses unstructured P2P network, the blockchain 2.0 uses structured P2P network and blockchain 3.0 uses both kinds of P2P network.

Consensus layer. The purpose of the consensus mechanism is to obtain an agreement on the impact of a transaction on a ledger update and to validate the transaction. The blockchain 1.0 uses PoW as its consensus algorithm, and the blockchain 2.0 also introduces algorithms such as PoS. Blockchain 3.0 adds more efficient algorithms such as PBFT and Raft.

Incentive layer. In the decentralized system, self-interested consensus nodes engage in to confirm data solely for the purpose of increasing private profits. [17]. Thus the this layer can help the system finally form a stable status, and the incentive layer is used in all three stages of the blockchain. However, there are some blockchain systems that do not have an incentive layer, such as the Hyperledger Fabric. The incentive layer contains different issuance mechanisms and distribution mechanisms.

Contract layer. All types of script code, algorithms, and more intricate smart contracts produced by the blockchain system are contained in the contract layer. The contract layer encapsulates various script codes, algorithms and smart contracts, so that the blockchain system can realize flexible programming and manipulation of data. In

fact, smart contracts were not really introduced until after blockchain 2.0, and blockchain 1.0 used a script scripting language.

Application layer. The application layer includes various applications on public blockchain, private blockchain and consortium blockchain, based on different categories of blockchain. As shown in Fig. 2.

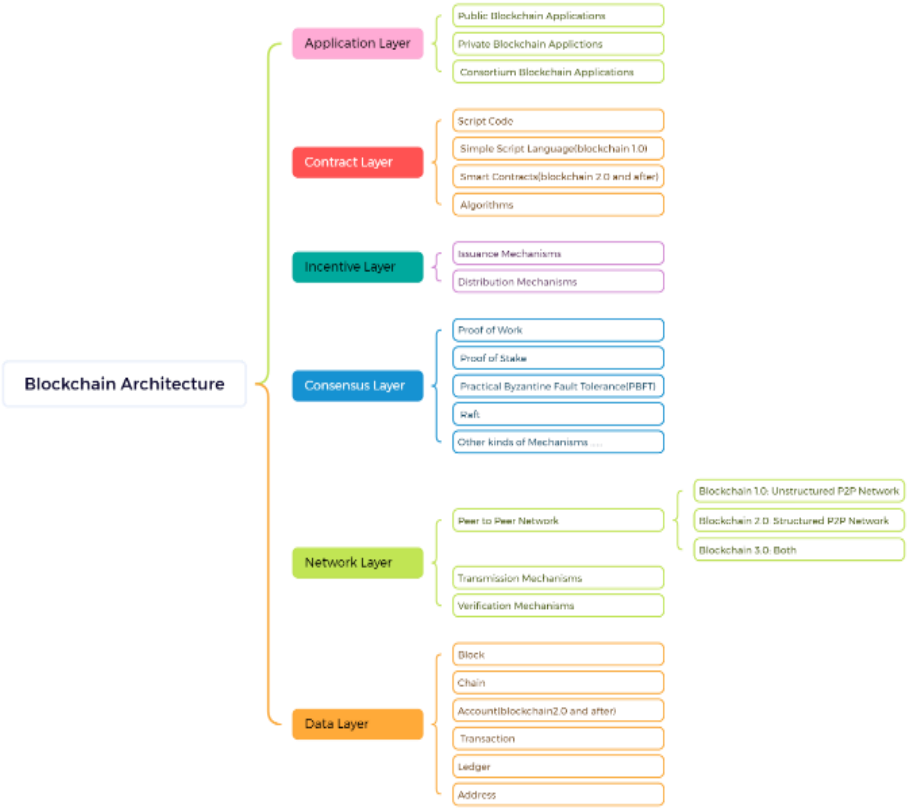

Fig. 2. Blockchain Architecture.

3 System Analysis and Application Research

The development and innovation of blockchain continue to advance, especially after the advent of the blockchain 3.0 era, its application has surpassed cryptocurrencies in the financial field and diversified expansion to all fields of society. Here are some examples of how blockchain can be used for authentication, cryptocurrency, supply chains, and the agricultural economy.

3.1 Identity Authentication System

Due to the decentralized, transparent, and immutable characteristics of blockchain, it is gradually being applied in the field of identity verification, demonstrating great

potential. Unlike normal confirmation systems, blockchain can confirm identities without storing users' personal privacy information. For example, Yasin and Liu created an identity management system that scores online, professional and personal reputations independently using blockchain technology. The system authenticates and protects the user's identity by analyzing the user's media and social activities.

When self-sovereign identity management is combined with blockchain technology, identity theft is typically virtually eliminated because no information about a central authority or other party can be deduced without the user's permission. In addition to the above, the potential of blockchain systems is constantly being explored and more practical applications in this area will emerge in the future.

3.2 Cryptocurrency

Cryptocurrencies are the initial application area of blockchain technology, and they are also the largest part of blockchain applications. Bitcoin and Ethereum, as mentioned earlier, are the most well-known examples of use cases in this filed.

There are hundreds of different cryptocurrencies on the market, they have different characteristics and mechanisms, play different roles. For instance, Curecoin employs its PoW to support research computations in protein folding, while Primecoin uses it to search for chains of prime numbers. These innovative cryptocurrencies use dual incentive approaches, which consumes energy while also bringing cryptocurrencies and valuable scientific data.

3.3 Supply Chain Applications

The supply chain is a key link for an enterprise's products to enter the market. In the process, participants may encounter issues such as supplier fraud, poor product quality, or excessive management costs, blockchain traceability can play an important role in this regard.

In addition, the combination of blockchain technology with IoT applications, such as RFID tags, sensors, etc., can track the location of products in the supply chain in real time, build trust among all parties, and improve delivery speed and material reliability. The application of this technology enhances the measurement objectives of supply chain management, such as quality, reliability and flexibility, and is carried out in a transparent manner.

3.4 Agricultural Economy

Blockchain technology is showing great potential in the field of agricultural economics. From improving the traceability of agricultural product quality and safety, to optimizing agricultural supply chain management, to improving farmland credit and financing, blockchain is bringing revolutionary changes to agriculture. For instance, Tian proposed the vision about the improved traceability system that can be applied on agricultural food production in response to food safety issues in Europe and China, based on blockchain. Through the unique characteristics of blockchain, the full tracking

of agricultural products can greatly improve their credibility and promote the development of agricultural economy.

4 Challenges

Although blockchain technology has significant advantages in the fields of data storage, identity authentication, and product traceability, and has been widely used, it still faces some challenges and limitations. This section lists the problems faced by most blockchain systems.

4.1 Performance and Scalability

Performance and scalability are key metrics to evaluate an application's ability to handle large-scale transactions. Due to the distributed architecture of the blockchain system, especially in most public blockchain, all nodes need to reach an agreement through a consensus mechanism to produce new blocks, which is usually a resource-intensive and time-consuming process. Such as Bitcoin, it generates blocks in an average of 10 minutes and has a poor throughput of 6–10 transactions per second (may be fewer depending on the network's complexity). At the same time, every transaction in Ethereum requires the payment of sufficient gas fees to ensure the success of the transaction. As a result, high transaction fees and transaction performance issues are currently a challenge for most blockchains, which limits their use cases, in other words, there are limitations to scalability.

In addition, blockchain system uses P2P networks and the performance is limited by network bandwidth and single-node performance. If developers want to break through these two limitations while maintaining decentralization, like improving the performance of most nodes, this will be a challenge.

4.2 Storage Cost

Blockchain’s traceability necessitates the system to store all historical transaction information, thereby continuously extending the entire blockchain and correspondingly increasing memory usage. Taking Bitcoin as an example, the memory usage of its blockchain has shown a rapid annual growth trend. According to statistics, as of January 2024, a full node in Bitcoin should at least has the memory of about 527 Gigabytes to store all necessary data [19]. This phenomenon reveals an important issue, that is, as time goes on, the storage overhead of the blockchain system gradually increases, which is undoubtedly an urgent problem to be solved. Therefore, how to effectively manage and control its storage overhead while maintaining the core characteristic of the blockchain — traceability, will be a significant challenge to blockchain technology.

4.3 Anonymity and Privacy

Transaction information in blockchain systems is transparent, meaning it is accessible to all participants. However, this also leads to issues with privacy security. For instance,

the initiators and recipients of transactions are typically presented in the form of addresses. This implies that attackers could potentially steal users' personal information by analyzing data such as IP addresses, thereby compromising anonymity. On the other hand, the anonymity provided by cryptocurrencies could lead to their use in concealing criminal clues or money laundering, making case tracking more difficult than usual. At the same time, there are currently no effective solutions to protect applications such as third-party wallets that store users' private keys and personal information. This means that information could also be leaked from these secondary channels.

4.4 Security and Fairness

In blockchain systems, all participants reach consensus through some mechanisms, like Bitcoin's PoW. However, this also brings about some security issues, the most well-known of which is the 51% attack, where an attack can occur when some miners control more than 50% of the computing power. On the other hand, the Proof of Stake (PoS) consensus mechanism used by Ethereum, which calculates the probability of block production based on the product of the amount of coins held and the holding time, can lead to centralization of stakes. Overall, the resource centralization problem caused by the consensus mechanism may cause the blockchain system to deviate from its original intention of decentralization, and thus be controlled or destroyed by certain organizations. This is an important issue that needs to be resolved in blockchain technology.

5 Conclusion

As an emergent technology, blockchain continues to evolve and exert influence across various sectors of society. Its distinctive characteristics offer potent solutions to prevalent challenges in contemporary applications, including identity verification and privacy protection. This paper provides a comprehensive analysis of blockchain's history, classifications, architecture, and principal applications. It delves deeply into the myriad challenges that blockchain currently confronts. Through a thorough examination of the entire blockchain ecosystem, this paper enables readers to gain a rapid and systematic understanding of the technology. Despite its numerous benefits, blockchain still encounters significant hurdles that must be overcome to facilitate broader adoption. Future research should focus on addressing these challenges and harnessing the technology to innovate and enhance existing applications. Moreover, with the continual emergence of new blockchain platforms and advancements, the application and comprehension of blockchain must also be dynamically updated and deepened. This ongoing adaptation will ensure that blockchain remains relevant and continues to drive technological innovation across various fields.

References

1. Gao, W., Hatcher, W. G., Yu, W.: A survey of blockchain: Techniques, applications, and

challenges. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN), IEEE, 1–11 (2018).
2. Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y.: A survey on blockchain technology: Evolution, architecture and security. IEEE Access 9, 61048–61073 (2021).
3. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008).
4. Buterin, V.: Ethereum white paper. GitHub repository 1, 22–23 (2013).
5. Hyperledger Project. Accessed: 2024-04-08.
6. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Vol. 310, No. 4, 1–4 (2016).
7. Zhu, X., Xu, H., Zhao, Z., & others: An Environmental Intrusion Detection Technology Based on WiFi. Wireless Personal Communications 119(2), 1425–1436 (2021).
8. Zheng, Z., Chen, & Wang, H.: Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services 14(4), 352–375 (2018).
9. Gamage, H. T. M., Weerasinghe, H. D., & Dias, N. G. J.: A survey on blockchain technology concepts, applications, and issues. SN Computer Science 1, 1–15 (2020).
10. Chaum, D.: Blind signatures for untraceable payments. In: Advances in Cryptology: Proceedings of Crypto 82, Springer US, Boston, MA, 199–203 (1983).
11. Sarmah, S. S.: Understanding blockchain technology. Computer Science and Engineering 8(2), 23–29 (2018).
12. Dai, W.: B-money. (1998).
13. Swan, M.: Blockchain: Blueprint for a new economy. O'Reilly Media, Inc. (2015).
14. Yuan, Y., & Wang, F.: Current Development and Future Prospects of Blockchain Technology. Journal of Automation 42(4), 481–494 (2016).
15. Yasin, A., & Liu, L.: An online identity and smart contract management system. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), IEEE, Vol. 2, 192–198 (2016).
16. 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), IEEE, 1–6 (2016).
17. Blockchain: Size of the Bitcoin blockchain from January 2009 to January 16, 2024. Accessed: 2024-04-08.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.