Blockchain Development

Siqi Xie[1,2], Jiahong Cai[1,2(✉)], Hangyu Zhu[1,2,3], Ce Yang[1,2], Lin Chen[1,2], and Weidong Xiao[4]

[1] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
{jiahongcai,yangce}@hnust.edu.cn
[2] Hunan Key Laboratory for Service Computing and Novel Software Technology, Xiangtan 411201, China
[3] Guangdong Financial High-Tech Zone "Blockchain +" Fintech Research Institute, Foshan 528253, China
[4] School of Software Engineering, Xiamen University of Technology, Xiamen 361024, China
xiaoweidong@xmut.edu.cn

Abstract. In recent years, blockchain research has set off an upsurge in academia, and it is called the next generation of value Internet. Because of its decentralization, anonymity, security, immutability, traceability and other characteristics, blockchain is gradually accepted and developed by people. With the deepening of research and the integration of technologies such as deep learning, blockchain has gradually been applied to various fields such as credit reporting, government, medical care, and industrial Internet of Things, not just the initial virtual currency field. This article mainly discusses the three important stages of blockchain public chain development, namely Bitcoin, Ethereum, and meta-verse, and introduces some basic supporting technologies of blockchain, as well as the research status and future trends of blockchain. Simple Analysis. By vertically introducing the development history of the blockchain, researchers can have a more concrete understanding of the status quo of the blockchain, and provide ideas for blockchain-related research.

Keywords: Blockchain · Bitcoin · Ethereum · Metaverse · Smart contracts

1 Introduction

Since the birth of blockchain, most countries had a positive attitude towards its research and industry development, with the United States legislating support, Canada having a positive view, and the Asia-Pacific region watching to explore the development of blockchain technology. In fact, blockchain is a database placed in a non-secure environment, which uses cryptography [1] to ensure that existing data cannot be changed, and consensus algorithms [2] to reach a consensus on new data. Only after Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System" [3] blockchain received widespread attention because the core idea of implementing Bitcoin is the blockchain, so Bitcoin is also called the blockchain 1.0 era by scholars. With the continuous research and development of applications, some problems gradually appeared in

M. Qiu et al. (Eds.): SmartCom 2022, LNCS 13828, pp. 597–606, 2023.
https://doi.org/10.1007/978-3-031-28124-2_56

the Bitcoin system, and to solve these problems, Ethereum was created, and this means that the blockchain officially entered the 2.0 era. The metaverse as the latest concept [4] has caused another lively discussion in the academic world [5, 6], and blockchain technology is one of the basic technologies to realize the meta-verse, and people's vision of blockchain 3.0 is that it can realize assets on the chain and construct various applications based on blockchain as the underlying framework to promote the large-scale creation in the fields of science, health [7], education, and images [8], so the metaverse whether the development of blockchain can bring it into the 3.0 era, everything is possible.

The remainder of this paper is organized as follows. Section 2 focuses on the birth of the blockchain and the basic components of the Bitcoin blockchain. Section 3 focuses on the features of the Ethereum blockchain and its improvement on the Bitcoin blockchain. Section 4 introduces the metaverse concept and the application of blockchain in the metaverse. Finally, Sect. 5 concludes the paper.

2 Blockchain 1.0 - Bitcoin

Scholars in different fields give different definitions of blockchain, which according to the literature [9] is a decentralized technology for transactions and data management. For users of the technology, blockchain represents a great improvement in the field of information collection, distribution, and governance [10]. The literature [11] compares blockchain to a tamper-proof digital ledger, implemented in a distributed manner. The literature [12] considers blockchain as a technology that makes the concept of a shared registry in distributed systems a reality in many application domains.

The concept of blockchain can be traced back to "How to Time-Stamp a Digital Document" written by Stuart Haber and W. Scott Stornetta in 1991 [13]. However, it was not until 2008 that the concept of blockchain appeared in the form of "block" and "chain" in Satoshi Nakamoto's article, attracting the attention of scholars from a new perspective of the application. This article focuses on Bitcoin, a virtual currency that he proposed. Bitcoin is not the earliest attempt at currency in the digital world. Virtual currencies such as Goofycoin and Zainucoin emerged before this, but they all ultimately failed. Until the emergence of Bitcoin, the problem of value and reliability was balanced with simple logic. A synthesis of the failures of previous virtual currencies sums up the following ideas.

1. Original currency transactions are simple and unlimited because they are made directly person-to-person, without the need for a bank-like third party. In fact, virtual currencies can also take advantage of this feature to simplify transactions, so the idea of decentralization emerged, directly turning the currency payment process into a "transaction" to a "transaction" form.
2. Digital products are replicable in nature and if they appear in monetary transactions, they are prone to double-spending problems, so to prevent "double-spending", it is better for everyone to witness it.
3. Since there is no third-party intervention and no concept of a balance wallet, a distributed consensus system is necessary to reach a consensus on the transaction witnessed by all. In order to prevent someone from being evil in the consensus

process, a penalty and reward mechanism was introduced to implement a consensus mechanism for many people—Proof of Work.

It was these seemingly simple, yet logical structures that led others to agree that the mechanism by which this currency operated was valid and reliable. Since the basis for Bitcoin's implementation of distributed consensus logic is the blockchain, there are great similarities between the two structures. Zhang et al. [14] summarize the structure of Bitcoin, dividing it into a data layer, a network layer, a consensus layer, a contract layer, and an application layer.

2.1 Data Layer

Block. A blockchain can be viewed as a distributed database that consists of individual blocks linked to each other. There are two main parts of the block, which are the block header and the block body. The block header stores the hash of the previous block, the hash of the content of the block body of the current block (the root of the Merkle tree), and the padding data Nonce. The block body contains the branch nodes of the Merkle tree, i.e., the specific transactions encapsulated in the block. As miners continue to experiment and over time, a continuously growing chain of blocks is created, and the constant updating of the chain represents the updating of the state of the Bitcoin ledger.

Timestamp. Blockchain is a chain structure. The process of chain formation is related to time stamps. The timing of each transaction is in order to prevent some illegal transactions. The timestamp identifies the time of each transaction and forms a chain relationship, its structure in Bitcoin is shown in Fig. 1.

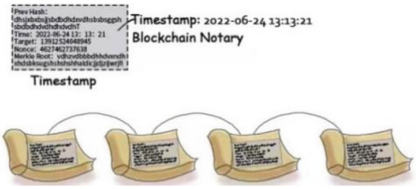

Fig. 1. Blockchain timestamp structure.

Hash Algorithm. The hashing algorithm used in the blockchain is SHA256. There is a probability of hash collision in the hashing algorithm, i.e., it is possible that there are two different numbers that have the same value obtained after calculation by the hash function [15]. However, since the output space of SHA256 is 2^{256}, with the existing computer computing power to forge a number and artificially create a hash collision unlikely, SHA256 can be used to verify whether a block in the blockchain has been tampered with. Hashing the transaction information in the block can form a summary of the block information, and when you need to verify the authenticity of the data, you can hash the transaction information again to determine whether there is a problem with the data.

2.2 Consensus Layer

Proof-of-Work. Bitcoin uses a Proof-of-Work (PoW) mechanism. Proof-of-Work is the mining process, which is simply the search for a number (Nonce) that will satisfy the target value by increasing the number of random bits in the block so that the zero bits when SHA256 is performed. The amount of work required is exponentially related to the number of required zero bits. The process of searching for Nonce is a continuous trial-and-error process, which requires CPU and power consumption. Finding a Nonce that meets the requirements represents the creation of a valid block. The target value is typically reset every 2016 blocks to ensure a frequency of one block generated every ten minutes.

Consensus Mechanism. In the traditional BFT consensus algorithm, the identity of each node must be known, but the nature of blockchain is fully public, everyone can participate in the system and can't reveal their identity, so BFT is no longer applicable. Blockchain is a timestamped server on a peer-to-peer basis, and proof-of-work solves the problem of identifying representatives in consensus decisions, in addition to preventing witch attacks and malicious chain generation. Since proof of work is essentially CPU arithmetic, a CPU represents one vote in a consensus decision. Most decisions are represented by the longest chain since a longer chain represents more workload proofs invested. As long as most of the CPU arithmetic is controlled by honest nodes, then honest chains will grow faster and outpace other competing chains.

2.3 Network Layer

Broadcast Mechanism. To give a macro summary of the Bitcoin transaction process. When a transaction is initiated, the initiator broadcasts it to all nodes, which receive the transaction in a block and perform a proof of work, and do not stop until one node finds the proof and broadcasts the block it is into all nodes. When the transactions in the block are verified by the nodes as all valid and unspent, the node accepts the block, and creates the next chain of acceptances to the block and uses the hash of the accepted block as the previous hash stored in the block header.

Validation Mechanism. In Bitcoin, since there is no concept of a wallet, this type of cryptocurrency ledger can also be seen as a state transition system, and the "state" refers to the current unused currency (UTXO), each UTXO contains a denomination and an owner, and the UTXO is updated after each transaction. UTXO is also one of the steps to verify the validity of the transaction. If two nodes include a block at the same time in this process, the remaining nodes must make a choice and continue mining. If the chain where the block is located is no longer the longest, the mined block will be invalidated.

2.4 Contract Layer

Incentives. All nodes are profit-driven, and the honesty of most nodes is critical to blockchain growth, so there must be incentives to ensure that nodes remain honest and

gain more than they would from a malicious attack. Node mining consumes CPU time and power, while the revenue is mainly through transaction fees. If the input value of a transaction is less than the output value, the difference is the transaction fee, which is included in the block containing the transaction. Also, every miner who successfully generates a block has the ability to include in the block a fee issued to itself, worth 12.5 BTC. if a malicious node, wants to get a fee by forging a transaction, then it will re-mine more blocks to make it more than the longest chain, thus making the forged transaction legitimate, which will undoubtedly consume more resources. Therefore, most nodes will still choose to be honest in order to gain revenue.

The final summary of the bitcoin transactions and the blockchain generation process is shown in Fig. 2.

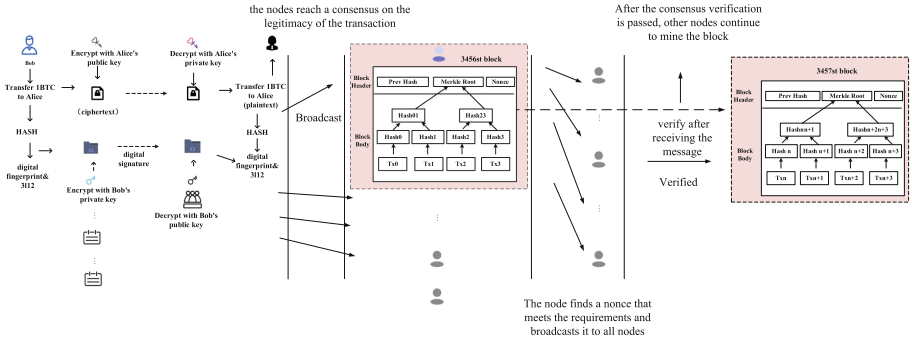

Fig. 2. Blockchain generation process.

3 Blockchain 2.0 - Ethereum

3.1 EThereum's Improvements to BItcoin's Logic

Bitcoin, as a virtual currency, is based on the core idea of a numerical exchange system. And while decentralization, consensus, hashing, and proof-of-work are all joint technologies adopted to allow this currency to be recognized and circulated. After the emergence of Bitcoin's decentralized consensus system, many currencies developed using this model have emerged, such as domain coins, colored coins, and meta-coins. However, Butlerin, the founder of Ethereum, argues that there are some problems with the scripts that implement this process of UTXO for verifying transactions in Bitcoin [16]. For example, lack of Turing completeness, lack of state, etc., so he proposed the Ethereum platform to address these problems and make some improvements.

Account. The "state" in Bitcoin consists of UTXO, while the "state" in Ethereum consists of accounts. It is divided into a contract account and an external account. Both of them contain transaction counters, Ethereum balances, storage for the account, and contract accounts additionally contain a contract code for the account. The external account has no code, the account holder can send messages to the contract account by creating

and signing transactions, and when the contract account receives the message, its code will be activated to perform the corresponding operation.

Trading. Since Ethereum is based on an account model, if a cryptocurrency transaction is initiated, then only the sufficiency of the balance on the Ethereum blockchain account needs to be verified, and the source of the Ethereum on the Ethereum blockchain does not need to be stated. This is also an improvement to the transaction-based model in Bitcoin. It is suitable for cases where transactions are large and complex. A transaction in Ethereum needs to contain the message recipient, a signature identifying the sender, the amount of Ethereum transferred, an optional data field, the maximum number of steps allowed for the transaction to execute, and a fee paid by the sender for each computational step. All but the last two concepts are fields that must be included in a cryptocurrency. The last two concepts are used to prevent certain nodes from maliciously provoking circular transactions or other arithmetic waste, and using them, a limit can be placed on the number of steps required for each transaction. Table 1 compares Bitcoin transactions with Ethereum transactions.

Table 1. Differences between Bitcoin and Ethereum.

Blockchain 1.0 Bitcoin (P2P)	Blockchain 2.0 Ethereum (end-to-end)
Decentralized Currency	Decentralized Contract Support
Based on the transaction model No concept of balance	Based on the account model Concept of balance
Go and check if the currently used bitcoin has already been used	Natural protection against a double-spend attack

3.2 Other Improvements in Ethereum

Ethereum not only improves on the Bitcoin blockchain but also establishes a protocol that can create decentralized applications that can be effectively used for small and micro applications and improve the interaction between programs. The proposal of smart contracts has brought the application of blockchain technology to a new level. Based on it, Ethereum is more like a development platform where users can write different applications through different smart contracts and allows everyone to write smart contracts through built-in Turing completeness, so Ethereum is a black box close to a Turing machine.

Smart Contracts. Smart contracts appeared before the birth of Bitcoin and almost simultaneously with the birth of the Internet. It was conceptualized by SZABO in 1995 [9], published on the website of the Extropy Institute. But the Internet environment at the time was not suitable for the development of smart contracts, they were never well used. Until the successful emergence of Bitcoin and the continuous development of blockchain technology provided good underlying support for the development of smart contracts.

Smart contracts applied on the blockchain are defined: smart contracts are event-driven, stateful programs that run on a replicable and shared ledger and are capable of holding the capital on the ledger [17]. In blockchain systems, smart contracts can run in three environments, namely embedded, virtual machine-based, and container-based [18].

Ethereum smart contracts are executed inside the Ethereum Virtual Machine EVM. The creation and use of a contract can be seen as a transaction process. Among them, creating a contract can be seen as a special kind of transaction process, where the creation function implements the creation of a new contract using a set of fixed parameters that produce a new set of states. The process is as follows.

$$(\sigma', g', A) \equiv \Lambda(\sigma, s, o, g, p, v, i, e) \tag{1}$$

Where σ' is the latest status, g' is the available gas value, A is the sub-state, σ is the system status, s is the transaction sender, o is the source account body, g is the available gas value, p is the gas price, v is the account balance, i is the initialization EVM code, e is the depth of the created contract stack.

Message. Another special feature of Ethereum is messages, which are executed in a similar but different way to "transactions". A transaction is initiated by a message sent from an external account and is real-name. A message is initiated by a contract to other contracts and is anonymous. It contains the sender of the message, the receiver of the message, the amount of Ethereum to be transferred with the message, an optional data field, and the maximum number of computation steps allowed for the message. The emergence of blockchain 2.0 - Ethereum has expanded the application of blockchain technology from cryptocurrency transactions to savings wallets [19], crop insurance [20], intelligent multi-signature escrow [21], cloud computing [22], and many more areas [23, 24].

4 Blockchain 3.0 - Metaverse

4.1 Introduction to the Concept of Metaverse

The metaverse as the latest buzzword has attracted a wide range of attention from industry and academia. The metaverse seamlessly merges the real and virtual worlds while allowing computers to perform many complex activities, including creation, presentation, entertainment, social networking, and trade, thus promising an exciting digital world. In exploring the metaverse, a better real world can also be transformed [25]. The concept of metaverse was first mentioned in a science fiction novel called Snow Crash [26], and the development of blockchain has made it possible to realize this world that exists only in science fiction. Some technology giants, such as Facebook [27], Epic [28], and Jingteng Tech, are working on the integration of the metaverse into their lives.

The image of users in the metaverse is a projection of humans in the real world, and as the metaverse develops, the image, creation, and consumption of humans in it will refine and influence the real world. In an idealized metaverse, transactions between virtual goods, such as clothes, cars, and real estate, can be realized, as well as the exchange of

virtual goods for real substances, in either form, it will affect the regular economy in the real world. The economic system in the metaverse can be divided into four parts: digital creation, digital assets, digital market, and digital currency. The article [25] summarizes them and compares their differences with the conventional economic system, as shown in Fig. 3.

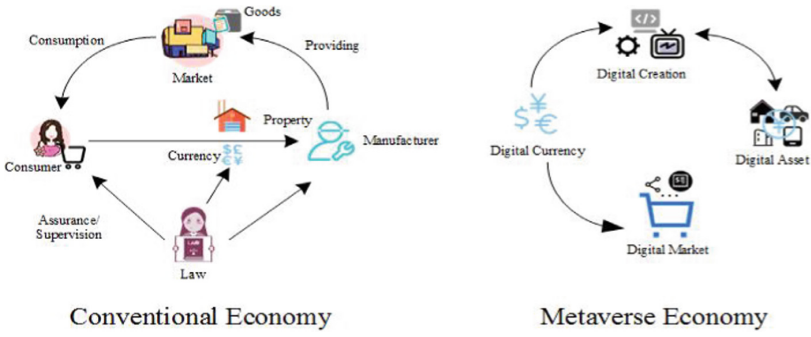

Fig. 3. Comparison of Traditional Economy and Metaverse Economy.

4.2 The Role of Blockchain in the Metaverse

If Ethereum is a black box close to a Turing machine, then by the 3.0 era blockchain will evolve into a Turing machine. Blockchain does three main things in this Turing machine. One is to ensure that most nodes are good [29]. Two is to maintain data security from being tampered with [30–32]. The third is to ensure that the transactions work correctly. The metaverse is a virtual world with an operation mechanism similar to the real world [33], a complete and self-consistent economic system, a complete industrial chain for producing and consuming digital products, and various transactions linking this virtual world together. The metaverse is positioned to be fair, notarized, and self-organizing, then the centralized economic system in the real world cannot function well in the metaverse due to the high transaction volume involved and the complexity of transactions. Thanks to the aid of big data techniques [34–36], the emergence of blockchain has broken the transaction barriers between regions in the circulation of money and opened the barriers in production, life, learning, and work so that the metaverse economic system is decentralized and the transactions using virtual images and virtual assets in the metaverse are legal and effective.

5 Conclusion

The development of blockchain technology from 1.0 to 3.0 is both the continuous improvement of technology and the continuous expansion of application scenarios, but there are also some problems during the development process, such as how to effectively communicate between different chains, the emergence of mining machines leading to

the concentration of arithmetic power, how to establish a perfect cross-chain protocol when one chain represents one currency, and how to use blockchain to handle massive transactions. For any technology, it will go through the process of gradually increasing the heat, reaching the peak, and then gradually decreasing and finally leveling off. At present, the research on selfish mining, fragmentation technology, and micropayment channel in blockchain had gradually matured, while the research on blockchain economy, decentralized finance, the integration of blockchain and 5G/6G, blockchain and edge computing were gradually rising in popularity. This also shows that blockchain technology is and will be changing various fields such as finance and communication. In addition to research on blockchain application areas, many scholars are also exploring the improvement aspects of blockchain based technologies, such as side-chain, lightning network, cross-chain, etc. are still in the popular stage of research.

References

1. Huang, Y., Liang, W., Long, J., et al.: A novel identity authentication for FPGA based IP designs. In: 17th IEEE TrustCom/BigDataSE, pp. 1531–1536 (2018)
2. Bach, L.M., Mihaljevic, B., Zagar, M.: Comparative analysis of blockchain consensus algorithms. In: 41st IEEE MIPRO, pp. 1545–1550 (201)
3. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Decent. Bus. Rev., 21260 (2008)
4. Wang, Y., Su, Z., Zhang, N., et al.: A survey on metaverse: fundamentals, security, and privacy. IEEE Commun. Surv. Tutor. (2022)
5. Liang, W., Tang, M., et al.: SIRSE: a secure identity recognition scheme based on electroencephalogram data with multi-factor feature. Comput. Electr. Eng. **65**, 310–321 (2018)
6. Xu, Z., Liang, W., Li, K.C., et al.: A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0. IEEE TII (2021)
7. Li, Y., Liang, W., Peng, L., et al.: Predicting drug-target interactions via dual-stream graph neural network. IEEE/ACM Trans. Comput. Biol. Bioinform. (2022)
8. Liang, W., Li, Y., Xie, K., et al.: Spatial-temporal aware inductive graph neural network for C-ITS data recovery. IEEE Trans. Intell. Transp. Syst. (2022)
9. Szabo, N.: Smart contracts: building blocks for digital markets. EXTROPY J. Transhumanist Thought (16) **18**(2), 28 (1996)
10. Bambara, J.J., Allen, P.R.: Blockchain. A practical Guide to Developing Business, Law and Technology Solutions. McGraw-Hill Professional, New York (2018)
11. Yaga, D., Mell, P., Roby, N., et al.: Blockchain technology overview. arXiv preprint arXiv: 1906.11078 (2019)
12. Belotti, M., Božić, N., Pujolle, G., et al.: A vademecum on blockchain technologies: when, which, and how. IEEE Commun. Surv. Tutor. **21**(4), 3796–3838 (2019)
13. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO 1990. NCD, vol. 537. Springer, , Heidelberg (1990). https://doi.org/10.1007/3-540-38424-3_32
14. Zhang, F., Shi, B., Jiang, W.: A review of key technologies and applications of blockchain. J. Netw. Inf. Secur. **4**(4), 22–29 (2018)
15. Rachmawati, D., Tarigan, J.T., Ginting, A.B.C.: A comparative study of message digest 5 (MD5) and SHA256 algorithm. J. Phys. Conf. Ser. **978**(1), 012116 (2018)
16. Buterin, V.: A next-generation smart contract and decentralized application platform. White Pap. **3**(37), 2–1 (2014)
17. Osterland, T., Rose, T.: Model checking smart contracts for ethereum. Pervasive Mob. Comput. **63**, 101129 (2020)

18. Jili, F., Xiaohua, L., Tiezheng, N., et al.: Overview of smart contract technology in blockchain system. Comput. Sci. **46**(11), 1–10 (2019)
19. Praitheeshan, P., Pan, L., Doss, R.: Security evaluation of smart contract-based on-chain ethereum wallets. In: Kutyłowski, M., Zhang, J., Chen, C. (eds.) NSS 2020. LNCS, vol. 12570, pp. 22–41. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-65745-1_2
20. Jha, N., Prashar, D., Khalaf, O.I., et al.: Blockchain based crop insurance: a decentralized insurance system for modernization of Indian farmers. Sustainability **13**(16), 8921 (2021)
21. Yang, X., Liu, M., Au, M.H., et al.: Efficient verifiably encrypted ECDSA-like signatures and their applications. IEEE TDSC **17**, 1573–1582 (2022)
22. Gai, K., Guo, J., Zhu, L., et al.: Blockchain meets cloud computing: a survey. IEEE Commun. Surv. Tutor. **22**(3), 2009–2030 (2020)
23. Liang, W., Yang, Y., Yang, C., et al.: PDPChain: a consortium blockchain-based privacy protection scheme for personal data. IEEE Trans. Reliab. (2022)
24. Liang, W., Xiao, L., Zhang, K., et al.: Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. IEEE Internet Things J. (2021)
25. Yang, Q., Zhao, Y., Huang, H., et al.: Fusing blockchain and AI with metaverse: a survey. IEEE Open J. Comput. Soc. **3**, 122–136 (2022)
26. Joshua, J.: information bodies: computational anxiety in Neal Stephenson's snow crash. Interdiscip. Lit. Stud. **19**(1), 17–47 (2017)
27. Meta, I.: A social technology company. Meta **12**(11), 2021 (2021)
28. Games, E.: Fortnite. Epic Games (2017)
29. Liang, W., Tang, M., Long, J., et al.: A secure fabric blockchain-based data transmission technique for industrial Internet-of-Things. IEEE TII **15**(6), 3582–3592 (2019)
30. Li, Y., Gai, K., et al.: Intercrossed access controls for secure financial services on multimedia big data in cloud systems. ACM Trans. Multimedia Comput. Commun. Appl. (2016)
31. Gai, K., Qiu, M., Elnagdy, S.: A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In: IEEE BigDataSecurity (2016)
32. Qiu, H., Dong, T., Zhang, T., Lu, J., Memmi, G., Qiu, M.: Adversarial attacks against network intrusion detection in IoT systems. IEEE IoT J. **8**(13), 10327–10335 (2020)
33. Kumar, P., Kumar, R., et al.: PPSF: a privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Trans. Netw. Sci. Eng. **8**(3), 2326–2341 (2021)
34. Hu, F., Lakdawala, S., et al.: Low-power, intelligent sensor hardware interface for medical data preprocessing. IEEE Trans. Inf. Technol. Biomed. **13**(4), 656–663 (2009)
35. Niu, J., Gao, Y., et al.: Selecting proper wireless network interfaces for user experience enhancement with guaranteed probability. JPDC **72**(12), 1565–1575 (2012)
36. Qiu, M., Xue, C., Shao, Z., Zhuge, Q., Liu, M., Sha, E.H.M.: Efficent algorithm of energy minimization for heterogeneous wireless sensor network. In: Sha, E., et al. (eds.) EUC 2006. LNCS, vol. 4096, pp. 25–34. Springer, Heidelberg (2006). https://doi.org/10.1007/11802167_5