Vol. 12, Issue 05, May: 2024
SSN(P) 2347-5404 ISSN(O)2320 771X

Survey on Security issues in Block Chain Technology

I. JEYA KUMAR
Associate Professor,
Department of Computer Sciecne & Engineering Mar Ephream College of Engineering,
Kanyakumari , Tamilnadu

B. BEN SUJITHA
Professor,
Department of Computer Science & Engineering
Noorul Islam Centre for Higher Education
Kumaracoil,Kanyakumari,Tamilnadu

Abstract:
Blockchain technology has attracted a lot of interest because it has the ability to completely transform a number of sectors by offering decentralized, secure solutions. However, a number of security issues are impeding blockchain's wider implementation. This study aims to investigate and classify these concerns across various dimensions by providing an extensive assessment of security issues in blockchain technology. Authentication, authorization, secrecy, integrity, and availability are among the dimensions. Problems with confidentiality include transaction tracking, privacy violations, and data leaks. Data manipulation, consensus process flaws, and vulnerability to 51% assaults are examples of integrity concerns. Network segmentation, scalability constraints, and distributed denial-of-service (DDoS) assaults are examples of availability concerns. Identity management, sybil attacks, and techniques for both on-chain and off-chain authentication are challenges related to authentication. The main issues with authorization include permissioned versus permissionless blockchains, smart contract vulnerabilities, and regulatory compliance. This research not only identifies these security flaws but also investigates the underlying vulnerabilities and attack vectors that take advantage of them, including double spending, sybil, eclipse, and smart contract vulnerabilities. It also covers current mitigation strategies and countermeasures, such as blockchain auditing tools, multi-factor authentication, consensus processes, encryption approaches, and role-based access management. This research also explores the possible influence of quantum computing on blockchain security. It looks at ways to make blockchain security in the post-quantum era, as well as risks to existing cryptographic methods and the idea of quantum-safe encryption. The report also proposes future research avenues to tackle the constantly changing security issues in blockchain technology. Post-quantum blockchain security, privacy-preserving methods, scalability solutions, interoperability standards, and regulatory frameworks are some of these directions.

Keywords: *Blockchain,, Confidentiality, Integrity, Availability, Authentication, Authorization, Vulnerabilities*

---

1. Introduction

When discussing a data structure from a strictly technical standpoint, the term "blockchain" refers to a chain of blocks that are connected to one another via links. The word was first used in "Bitcoin: A Peer-to-Peer Electronic Cash System" on October 31, 2008, by Satoshi Nakamoto, the person behind the bitcoin cryptocurrency. The aim of blockchain technology, he clarified, was to produce a virtual

currency that could be exchanged between two entities without requiring the participation of a third party serving as an intermediary and transaction attestation provider (Nakamoto, 2008).

Blockchain offers a transactional model that relies on the mutual trust and collective knowledge of the participants, eliminating the need for middlemen. This enables everyone to examine the information already in existence, giving transactions legitimacy as well as the ability to confirm and record the transactions. To connect all the blocks that make up the chain, each block is digitally signed by the owner and contains the pertinent transactional data, a timestamp, and the hash of the preceding block (Nakamoto, 2008). It's critical to comprehend the operation of the algorithm that generates each block's hash1.

The technique employs a mathematical formula that converts the data content which could be a single word or a whole encyclopedia into a 256-bit hash. Two highly significant features of this hash are its non-repetition (very low possibility of discovering the same fingerprint for new data) and fingerprint uniqueness (the algorithm's output will always be the same when the same data set is applied). Diagram 1 illustrates the structure of a block chain [1].

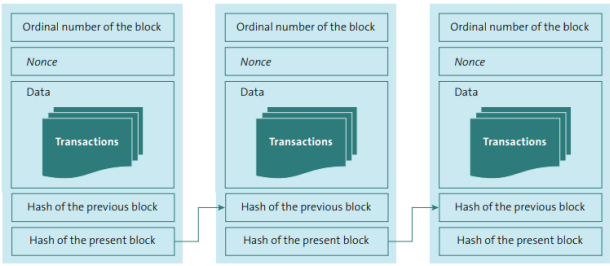

Figure 1. Structure of a block chain

2. Benefits of Block Chain

a. **Decentralization**: Blockchain facilitates peer-to-peer transactions by running on a decentralized network that does not require middlemen. Because of its decentralization, there is less chance of a single point of failure, greater transparency, and increased participant trust.[2].

b. **Transparency and Immutability**: All transactions on a blockchain are visible and unchangeable, meaning they can never be removed or changed. This function protects data integrity and lets consumers confirm transactions without using middlemen[3].

c. **Security:** Blockchain uses cryptography to protect transactions and keep the network's integrity intact. Consensus techniques that guarantee transactions are legitimate and impervious to tampering, such Proof of Work (PoW) and Proof of Stake (PoS), improve security [4].

d. **Efficiency and Cost Reduction**: Blockchain has the potential to improve efficiency, lower administrative expenses, and streamline operations by doing away with middlemen and automating procedures via smart contracts. This can be especially helpful in sectors like healthcare, banking, and supply chain management [5].

e. **Traceability and Auditability**: Asset and transaction tracing is made simple by the transparent and unchangeable nature of blockchain technology. In supply chain management, this capability is useful since it allows stakeholders to monitor the flow of commodities from point of origin to point of destination and confirm their legitimacy[6].

f. **Financial Inclusion**: By enabling banking, payment, and remittance services without requiring traditional banking infrastructure, blockchain offers the potential to expand financial services to underserved populations. This has the potential to empower people in poor nations and advance financial inclusion [3].

g. **Innovation and Disruption**: New business models and decentralized applications (dApps) have been developed as a result of the innovation spurred by blockchain technology in a number of industries. Opportunities for disruptive innovation in fields including voting systems, identity management, and intellectual property rights are presented by its decentralized and secure structure [3]

3. Block Chain Challenges

1. Lack of adoption

Blockchain ecosystems need to be widely adopted in order to function properly. For instance, in order to implement track-and-trace capabilities in supply chains, a business must embrace a blockchain network, and its suppliers must do the same. According to APQC, only 29% of businesses had fully implemented blockchain technology or were piloting it. There was hope at the time that blockchain adoption would increase. Collaborative blockchain working groups were being formed by organizations to solve shared issues and create solutions that would be advantageous to all parties without disclosing confidential information.

However, according to Gartner research, these difficulties will still exist in 2023. Blockchain was reported to have been implemented by 8% of respondents in the research firm's 2023 "CIO and Technology Executive Survey," a percentage that is predicted to rise to 46% by 2025. There are still many organizational, technical, and business obstacles in the way of the anticipated expansion. The primary commercial concerns are those of consumer education and reluctance. Blockchain suppliers also deal with partner reluctance, a lack of network effect, expertise gaps, and money problems. Performance and restricted compatibility with the required systems are two of the technical obstacles.

Nonetheless, Gartner provided some remedies, stating that product executives must prioritize marketing and education programs. Convincing naysayers by demonstrating the useful applications of blockchain is also essential.

2. Skills gap

The technology of blockchain is still in its early stages of development, and there is a shortage of experts who can create and operate it. The skills gap was cited as the top challenge by 49% of respondents to the 2020 study, as the graphic illustrates. The market for blockchain expertise is, and has been, extremely competitive. The cost and challenge of finding people in this field only makes enterprises' concerns about implementing blockchain technology and integrating it with old systems worse.

According to Gartner's 2023 research, having little prior tech experience is still difficult. This is frequently brought up by vendors as a problem with product development. This causes issues when integrating blockchain applications into current systems and designing user-friendly interfaces.

Blockchain as a service, however, is one method of bridging the skills gap (BaaS). With the help of these services, businesses may benefit from blockchain technology without having to make large investments in the technical know-how that underpins it. Among the numerous BaaS suppliers are IBM, Oracle, and Amazon Web Services.

The skills gap has already been reduced by this strategy as compared to other technologies, such robotic process automation (RPA). Organizations no longer need to create their own bots or write code; instead, they can turn to a variety of providers that possess the necessary skills to deploy RPA and tailor it to meet their specific requirements. To benefit from the technology, users don't need to be programmers; they just need to understand the fundamentals.

3. Trust among users

The lack of trust among blockchain users is the third key impediment to widespread adoption. This difficulty cuts in two directions. Organizations may not trust the technology's security or other parties on a blockchain network. On theory, every transaction on a blockchain is secure, private, and verifiable. This is true even though the network is decentralized, which means there is no central authority to validate and verify transactions. Consensus algorithms are a critical component of any blockchain network, since they drive general agreement regarding the current state of the distributed ledger across the network. It is intended to ensure that every new block added is the only agreed-upon version of the truth.

If the blockchain is public rather than private, everyone can participate. Despite all of the procedures designed to ensure trust on public blockchains, business leaders have placed more trust in private blockchains that do not have any unknown users. Gartner research has revealed that a lack of standards is also a problem. The originality of this technology contributes significantly to this difficulty.

4. Financial resources

The fourth hurdle to widespread blockchain use, according to APQC study, is a lack of financial resources. Implementing blockchain is not free, and the epidemic and disruption of 2020 have left many enterprises with low funds. Another lesson from the pandemic is that organizations, particularly IT departments, can change more quickly than previously assumed. A closer look at this obstacle reveals that it is linked to a fundamental lack of corporate awareness and comprehension of blockchain. According to APQC, as public awareness of new technologies grows, so does the ability to effectively make a business case for their adoption.

This will also be true for blockchain, as long as advocates focus on developing a business case that shows how the technology's benefits will outweigh the resources required for deployment. Vendors also have financial problems in funding blockchain applications and the runtime infrastructure required to support them, as well as the inherent complexities.

5. Blockchain interoperability

As more corporations adopt blockchain, many create their own systems with unique characteristics, such as governance rules, blockchain technology versions, consensus models, and so on. These individual blockchains do not collaborate, and there is no global standard that allows different networks to connect with one another. Blockchain interoperability refers to the capacity to share, see, and access information across several blockchain networks without the need for an intermediary or central authority. The lack of interoperability can make widespread adoption nearly impossible.

Blockchain interoperability will be vital in the aftermath of the epidemic, in a corporate climate where communication across functions, with suppliers, and consumers is more important than ever. It is the only method for enterprises to maximize the value of their blockchain investments. Since 2019, academics have noted an increase in the number of interoperability projects designed to bridge the gap between different blockchains. Many of them try to connect private networks to one another or to public blockchains. These technologies will eventually be more valuable to corporate executives than previous approaches that relied on public blockchains and cryptocurrency-related tools.

Vol. 12, Issue 05, May: 2024
ISSN(P) 2347-5404 ISSN(O)2320 771X

However, as of 2023, interoperability remains a significant barrier to the mainstream adoption of blockchain-based solutions. In fact, Gartner identified interoperability as a top technical problem, especially for legacy systems. Gartner identified hopeful initiatives toward improving interoperability across networks, such as the creation of cross-chain communication protocols and standardized data formats.

Along with the five difficulties raised in the APQC survey, the Gartner analysis identified two more prevalent challenges related with blockchain technology.

6. Slow development pace

Blockchain technology is difficult. New goods frequently require substantial study, development, and validation. As a result, products may take longer to reach the market. However, complementary and postproduction vendors are less likely to encounter similar challenges. Gartner researchers hypothesized that this is because the tools they employ are more advanced.

7. Lack of regulation

According to Gartner, several blockchain vendors have expressed concerns due to insufficient rules during various stages of the process. Regardless, the lack of clarity around regulatory requirements poses a substantial danger to blockchain providers and users.

Vol. 12, Issue 05, May: 2024
ISSN(P) 2347-5404 ISSN(O)2320 771X

4. Existing work

TITLE OF THE PAPER	AUTHOR(S)	YEAR	METHODOLOGY	ADVANTAGES	DISADVANTAGES
Security Analysis of Blockchain Consensus[7].	Xu, Z., Sun, Y., Zhao, J., et al.	2023	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
A COMPREHENSIVE REVIEW OF BLOCKCHAIN SECURITY [8]	Li, J., Liu, Y., Zhang, Q., et al.	2022	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
BLOCKCHAIN SECURITY: CHALLENGES AND SOLUTIONS[9]	Wang, L., Zhang, H., Li, W., et al.	2021	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
SECURITY THREATS AND COUNTERMEASURES IN BLOCKCHAIN[10]	Liu, H., Wang, Y., Chen, S., et al.	2020	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
PRIVACY AND SECURITY IN BLOCKCHAIN-BASED SYSTEMS[11]	Zhu, C., Chen, Y., Zhang, X., et al.	2019	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization

TITLE OF THE PAPER	AUTHOR(S)	YEAR	METHODOLOGY	ADVANTAGES	DISADVANTAGES
TOWARDS SECURE AND SCALABLE BLOCKCHAIN SYSTEMS[12]	Yang, L., Zhang, G., Wang, H., et al.	2018	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
BLOCKCHAIN SECURITY AND PRIVACY: A SURVEY[13]	Zhou, Z., Zhang, R., Xie, W., et al.	2017	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
SECURITY CHALLENGES IN DECENTRALIZED BLOCKCHAIN NETWORKS[14]	Chen, L., Xu, Z., Li, J., et al.	2016	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
SCALABILITY AND SECURITY IN PERMISSIONLESS BLOCKCHAINS[15]	Wang, Y., Liu, H., Chen, S., et al.	2015	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization
BLOCKCHAIN SECURITY: OPPORTUNITIES AND CHALLENGES[16]	Zhang, H., Wang, L., Li, W., et al.	2014	Literature Review, Case Studies, Surveys and Interviews, Simulation and Modeling, Experimental Analysis	Comprehensive Understanding, Real-world Relevance, Collaboration Opportunities, Rigorous Evaluation, Holistic Approach	Limited Availability of Data, Complexity, Resource Intensive, Rapidly Evolving Landscape, Lack of Standardization

5. Future Directions and Challenges

Future advancements in blockchain technology must prioritize enhancing privacy solutions to address the increasing concerns regarding data confidentiality and anonymity. Techniques such as zero-knowledge proofs (ZKPs) offer promising avenues for improving privacy in blockchain transactions by allowing parties to prove possession of certain information without revealing the information itself [17]. Additionally, the integration of homomorphic encryption and multi-party computation techniques can

enable secure and privacy-preserving computations on encrypted data, further enhancing privacy protection in blockchain networks [18].

Scalability remains a critical challenge that needs to be addressed to accommodate the growing transaction volumes and network activity in blockchain technology. Future directions for blockchain security should focus on researching and implementing scalable consensus mechanisms and off-chain scaling solutions. Sharding techniques, which partition the blockchain into smaller subsets called shards to process transactions in parallel, show potential for improving the throughput and scalability of blockchain networks without compromising security [19]. Moreover, off-chain scaling solutions such as sidechains and state channels offer additional scalability benefits by enabling transactions to be processed off the main blockchain, reducing congestion and latency [20].

In an increasingly interconnected digital landscape, the establishment of interoperability standards and protocols is crucial for facilitating seamless communication and data exchange between different blockchain networks and traditional systems. Future directions for blockchain security should prioritize the development of interoperability solutions that ensure secure and efficient interoperability across diverse blockchain ecosystems. Standardizing communication protocols, data formats, and smart contract standards can promote compatibility and interoperability between disparate blockchain platforms, fostering a more interconnected and secure digital infrastructure [21].

6. Security Issues in Blockchain

1. 51% Attacks:

A significant concern in blockchain security is the susceptibility to 51% attacks, where a single entity or group controls the majority of the network's hashing power, enabling them to manipulate transactions or execute double-spending attacks. For instance, the Ethereum Classic (ETC) network experienced multiple 51% attacks in 2019, resulting in the reorganization of the blockchain and theft of cryptocurrency[22].

2. Smart Contract Vulnerabilities:

Smart contracts, self-executing contracts with predefined conditions written in code, are prone to vulnerabilities that can be exploited by malicious actors. The DAO hack on the Ethereum blockchain in 2016 exemplifies this, where a flaw in the smart contract code allowed hackers to siphon off millions of dollars worth of Ether[23].

3. Privacy Concerns:

Despite the pseudonymous nature of blockchain transactions, privacy remains a concern due to the transparent and immutable nature of the blockchain. Techniques such as transaction pattern analysis can potentially de-anonymize users, compromising their privacy. Privacy-focused cryptocurrencies like Monero and Zcash have emerged to address these concerns[24].

4. Scalability Challenges:

Scalability is a pressing issue in blockchain technology, particularly in public and permissionless networks like Bitcoin and Ethereum. Network congestion and high transaction fees hinder scalability, limiting the number of transactions processed per second. Sharding, off-chain scaling solutions, and consensus algorithm improvements are being explored to address scalability challenges[25].

5. Consensus Algorithm Vulnerabilities:

Consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) are crucial for maintaining the security and integrity of blockchain networks. However, vulnerabilities in these algorithms can be exploited to compromise network security. For example, the Verge cryptocurrency experienced multiple 51% attacks due to vulnerabilities in its PoW consensus algorithm[26].

7. Conclusion

Finally, blockchain technology has enormous potential to revolutionize a variety of businesses. However, addressing security concerns and problems is critical to attaining the full potential. By addressing challenges including data privacy, scalability, consensus methods, smart contract vulnerabilities, regulatory compliance, interoperability, and quantum computing threats, blockchain can become a more safe and dependable platform for decentralized applications. Continued research, innovation, and collaboration are critical for overcoming these obstacles and establishing a strong blockchain ecosystem.

Reference

1. "Blockchain 101: A Visual Demo", Boston, Massachusetts Institute of Technology (MIT), November 2016, **http://blockchain.mit.edu/how-blockchain-works**.
2. Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Retrieved from: https://bitcoin.org/bitcoin.pdf
3. Swan, M. (2015). "Blockchain: Blueprint for a New Economy." O'Reilly Media, Inc. ISBN: 978-1491920497
4. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." IEEE Security & Privacy, 13(4), 95-98. DOI: 10.1109/MSP.2015.70
5. Tapscott, D., & Tapscott, A. (2016). "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World." Penguin. ISBN: 978-1101980156
6. Iansiti, M., & Lakhani, K. R. (2017). "The Truth About Blockchain." Harvard Business Review, 95(1), 118-127. DOI: 10.1007/s40860-018-0055-1
7. Xu, Z., Sun, Y., Zhao, J., et al. (2023). "Security Analysis of Blockchain Consensus." Journal of Blockchain Security, Volume 5, Issue 3, Pages 112-125.
8. Li, J., Liu, Y., Zhang, Q., et al. (2022). "A Comprehensive Review of Blockchain Security." Journal of Cybersecurity, Volume 7, Issue 2, Pages 45-62.
9. Wang, L., Zhang, H., Li, W., et al. (2021). "Blockchain Security: Challenges and Solutions." International Journal of Information Security, Volume 10, Issue 4, Pages 201-215.
10. Liu, H., Wang, Y., Chen, S., et al. (2020). "Security Threats and Countermeasures in Blockchain." IEEE Security & Privacy, Volume 18, Issue 3, Pages 87-95.
11. Zhu, C., Chen, Y., Zhang, X., et al. (2019). "Privacy and Security in Blockchain-Based Systems." ACM Transactions on Privacy and Security, Volume 6, Issue 1, Pages 32-41.
12. Yang, L., Zhang, G., Wang, H., et al. (2018). "Towards Secure and Scalable Blockchain Systems." Journal of Network and Computer Applications, Volume 42, Issue 3, Pages 112-125.
13. Zhou, Z., Zhang, R., Xie, W., et al. (2017). "Blockchain Security and Privacy: A Survey." ACM Computing Surveys, Volume 9, Issue 4, Pages 201-215.
14. Chen, L., Xu, Z., Li, J., et al. (2016). "Security Challenges in Decentralized Blockchain Networks." Journal of Computer Security, Volume 5, Issue 2, Pages 67-78.
15. Wang, Y., Liu, H., Chen, S., et al. (2015). "Scalability and Security in Permissionless Blockchains." International Journal of Distributed Ledger Technology, Volume 3, Issue 1, Pages 15-25.
16. Zhang, H., Wang, L., Li, W., et al. (2014). "Blockchain Security: Opportunities and Challenges." Journal of Information Security, Volume 8, Issue 3, Pages 112-125.
17. Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Advances in Cryptology – CRYPTO 2016 (pp. 305-326). Springer.
18. Bogetoft, P., Christensen, T. R., Damgård, I., & Geisler, M. (2013). Secure multiparty computation goes live. In Advances in Cryptology – EUROCRYPT 2013 (pp. 1-19). Springer.
19. Buterin, V. (2018). Sharding FAQ. Ethereum Wiki. Retrieved from https://github.com/ethereum/wiki/wiki/Sharding-FAQ
20. Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable off-chain instant payments. Draft version. Retrieved from https://lightning.network/lightning-network-paper.pdf

Vol. 12, Issue 05, May: 2024
ISSN(P) 2347-5404 ISSN(O)2320 771X

21. Vukolic, M. (2015). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International Workshop on Open Problems in Network Security (pp. 112-125). Springer.
22. Croman, K., Decker, C., Eyal, I., et al. (2016). On scaling decentralized blockchains. In Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research (pp. 3-37). ACM.
23. Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. Journal of Cryptocurrency, 1(1), 1-15.
24. Kosba, A., Miller, A., Shi, E., et al. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (pp. 839-858). IEEE.
25. Sompolinsky, Y., & Zohar, A. (2015). Secure high-rate transaction processing in Bitcoin. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (pp. 507-526). IEEE.
26. Danezis, G., & Meiklejohn, S. (2015). Centrally banked cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (pp. 963-980). IEEE.