Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.040596

REVIEW

Blockchain Security Threats and Collaborative Defense: A Literature Review

Xiulai Li[1,2,3,4], Jieren Cheng[1,3,*], Zhaoxin Shi[2,3], Jingxin Liu[2,3], Bin Zhang[1,3], Xinbing Xu[2,3], Xiangyan Tang[1,3] and Victor S. Sheng[5]

[1]School of Computer Science and Technology, Hainan University, Haikou, 570228, China

[2]School of Cyberspace Security, Hainan University, Haikou, 570228, China

[3]Hainan Blockchain Technology Engineering Research Center, Hainan University, Haikou, 570228, China

[4]Hainan Hairui Zhong Chuang Technol Co. Ltd., Haikou, 570228, China

[5]Department of Computer Science, Texas Tech University, Lubbock, 79409, USA

*Corresponding Author: Jieren Cheng. Email: cjr22@163.com

Received: 24 March 2023 Accepted: 25 May 2023 Published: 08 October 2023

ABSTRACT

As a distributed database, the system security of the blockchain is of great significance to prevent tampering, protect privacy, prevent double spending, and improve credibility. Due to the decentralized and trustless nature of blockchain, the security defense of the blockchain system has become one of the most important measures. This paper comprehensively reviews the research progress of blockchain security threats and collaborative defense, and we first introduce the overview, classification, and threat assessment process of blockchain security threats. Then, we investigate the research status of single-node defense technology and multi-node collaborative defense technology and summarize the blockchain security evaluation indicators and evaluation methods. Finally, we discuss the challenges of blockchain security and future research directions, such as parallel detection and federated learning. This paper aims to stimulate further research and discussion on blockchain security, providing more reliable security guarantees for the use and development of blockchain technology to face changing threats and challenges through continuous updating and improvement of defense technologies.

KEYWORDS

Blockchain; threat assessment; collaborative defense; security evaluation

1 Introduction

The growth and innovation of the digital economy have been greatly aided by the development of blockchain technology [1]. Blockchain technology is a young technology that has already found extensive use in a variety of industries, including healthcare, copyright protection, the Internet of Things, supply chain management, and finance. Yet, as the size of blockchain systems continues to grow and there are more and more application scenarios, the security issues they confront are getting more significant and complex. Blockchain systems' security and stability have been gravely endangered by many assaults and threats, such as double-spend attacks, 51% attacks, and smart contract vulnerabilities, which are frequently present in real deployments.

The paper [2] aimed to explore blockchain security threats, highlight the privacy requirements of current applications, and outline their difficulties while offering insights on how these difficulties can be solved through blockchain technology to provide a thorough survey of blockchain technology. However, it does not provide specific examples or case studies to illustrate the successes and limitations of using blockchain technology for real-world applications. In the paper [3], the development framework, architecture, security concerns, comparative study of the framework, classification of the consensus method, security threats, and cryptographic primitives currently employed in blockchain technology were all thoroughly examined. It does not explain how these technologies apply to specific sectors or use cases. The paper [4] addressed the blockchain development platforms and technologies as well as a comparative examination of the blockchain consensus algorithms offered for various application kinds. It does not evaluate the actual implications and constraints of deploying these technologies in diverse sectors or use cases. To study the performance of blockchain-enabled consensus algorithms, the paper [5] gives a thorough taxonomy for blockchain performance research that tries to spot overlaps and differences as well as existing work on simulators and benchmarking systems.

As shown in Fig. 1, many security precautions must be implemented to address the security vulnerabilities with blockchain systems. Multi-node collaborative defense is a crucial strategy among these countermeasures. The blockchain system's security and stability can be increased by relying on numerous nodes to monitor, back up, achieve consensus, and upgrade the blockchain system for defense. Multi-node collaborative defense, as opposed to the conventional single-node defense method, may more effectively coordinate the resources between each node and cooperatively maintain the security of the blockchain. As a result, the multi-node collaborative defense has emerged as one of the key tools for ensuring blockchain security, where the comparison among different defensive measures is listed in Table 1. Single-measure defense is prone to attacks and unreliable. Attackers can quickly exploit defense flaws to compromise them. Multi-measure cooperative defense uses numerous defense systems concurrently. This can guard against numerous threats, but it requires a lot of resources and experience to implement. Single-node defense, which secures blockchain nodes, is ineffective since nodes cannot function after downtime. Attacks can occur if a node fails. Multi-node collaborative defense coordinates nodes to defend against attacks. This strategy can improve security, but it is complicated and requires node coordination.

The multi-node collaborative defense of blockchain will be examined and analyzed in this study, along with the security risks that blockchain is subject to, the collaborative defense's technical tools, and security evaluation techniques. Multi-node collaborative defense's ideas and technical implementation will be covered, along with an analysis of its benefits and drawbacks and a summary of successful real-world implementations. Also, we hope that the work of this article will stimulate additional study and conversation on blockchain security, allowing for the provision of more reliable security assurance for the use and advancement of blockchain technology.

2 Overview of Blockchain Security Threats

2.1 Classification of Blockchain Security Threats

The network layer, protocol layer, and application layer are the three main categories into which the security risks of blockchain technology can be classified.

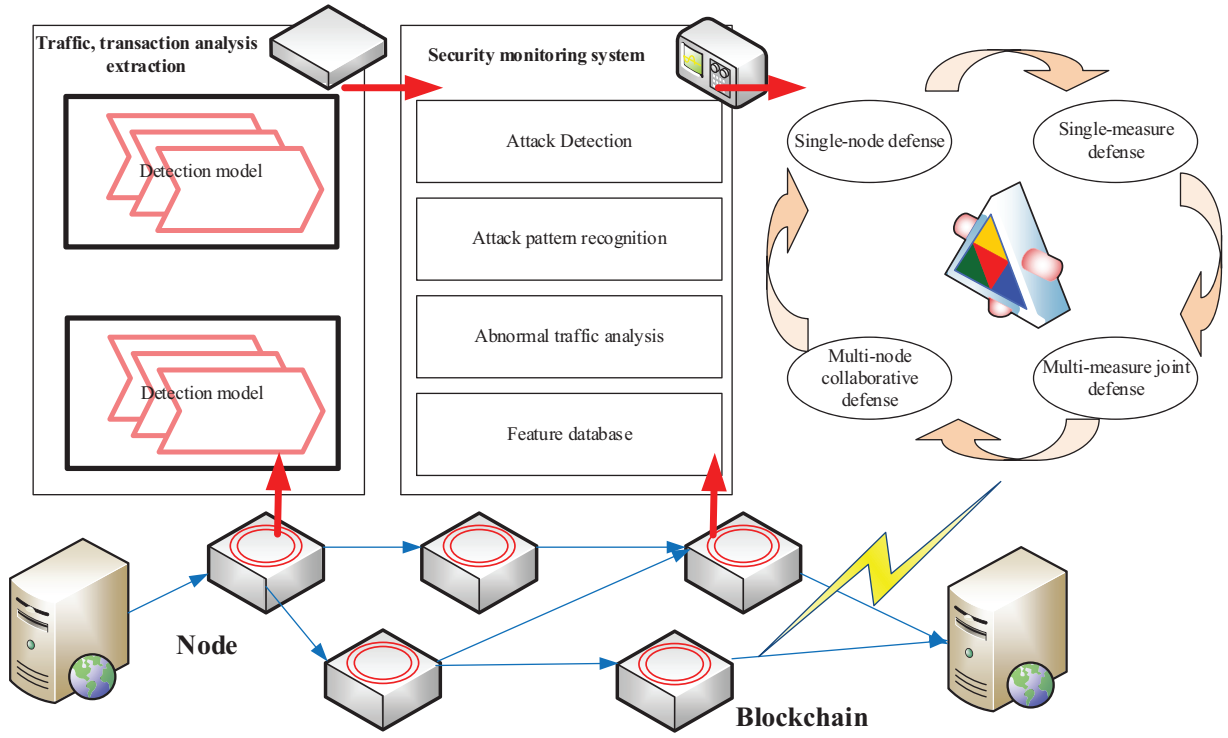

Figure 1: Security precautions in blockchain systems

Table 1: Comparison of different defensive measures

Defensive measures	Description	Pros	Cons	Applicable scenarios
Single-measure defense [6]	Use a single technique or measure, such as cryptographic algorithms or authentication	Simple and easy to implement	Vulnerable to attack, unreliable defense	A single defense for low-risk environments and simple systems provides the basic security for these systems. For example, for a website that is only used for presentation, using basic authentication measures may be sufficient.
Multi-measure joint defense	Use multiple technologies or measures to use together, such as cryptographic algorithms, authentication, multi-signature, etc.	Attacks are difficult and the defense effect is more reliable	Complex and costly implementation	Multiple defenses for complex systems and high-risk environments provide a higher level of security. For example, financial institutions need to use multiple defense measures, including access control, encryption, auditing, and intrusion detection, to improve their security and protect customers' property and information.

(Continued)

Table 1 (continued)

Defensive measures	Description	Pros	Cons	Applicable scenarios
Single node defense [7]	Defense against a single node, If running in a physically isolated environment	High security, not vulnerable to attack	Nodes cannot continue to work after downtime	It is a kind of Cybersecurity defense for PCs, mobile devices, and small businesses or organizations. For individual users or small businesses, a single-node defense solution is sufficient to provide basic security, including firewalls, intrusion detection, and antivirus software.
Multi-node collaborative defense [8]	Multiple nodes work together for defense, such as the Byzantine fault-tolerant algorithm	High security, even if individual nodes are attacked, it will not affect the entire system	The implementation is complex and requires coordination of the behavior of multiple nodes	Suitable for cybersecurity defenses of large enterprises or organizations and security defenses in cloud computing environments. In the network environment of a large enterprise or organization, multi-node defense is required to secure the network. In a cloud computing environment, the security of the entire cloud computing environment can be improved by using multiple virtual machines or containers to run different security software, such as antivirus software, intrusion detection systems, etc.

(1) Security threats in the network layer

Network layer security threats mainly include man-in-the-middle attacks, Distributed Denial of Service (DDoS) attacks, replay attacks, and network partition attacks. An attack known as a "man-in-the-middle" occurs when a hacker tampers with network communication packets by impersonating nodes to get false information or carry out harmful deeds. Man-in-the-middle attacks in the blockchain system can result in issues including tampering with blockchain data and double-spending attacks. DDoS attacks are when attackers overload or crash network systems by sending a large number of requests to nodes in the network. In a blockchain system, DDoS attacks can cause network delays and nodes to become unresponsive, affecting the stability and availability of the blockchain system. If T_r is used to represent the response time of the resource consumer, and T_s represents the speed at which the attacker's request is sent, a distributed denial-of-service attack (DDoS) can be represented as:

$$T_r > T_s \tag{1}$$

that is, the system cannot respond to a legitimate user's request [9]. An attacker who acquires some lawful communication packets from the network and replays them to the target node can gain unauthorized access control. This is known as a replay attack. Replay attacks have a particularly

negative effect on blockchain systems since they might result in double-spend assaults against the system [10]. A network partitioning assault occurs when an attacker takes control of a few network nodes, prevents them from interacting with other nodes, splits the network into multiple separate sub-networks, and eventually results in network splitting. Network partitioning attacks are a particularly serious issue in distributed systems because they might cause the system to have a Byzantine failure, or an inability to reach a consensus [11].

(2) Security threats in the protocol layer

Double Spending Attack: This is when a hacker sends two identical transactions to the blockchain network to deceive the system and earn additional cryptocurrency for himself. If the attacker is strong enough, they can add a second transaction to a blockchain that is lengthier than the original one, confirming the second one while nullifying the first, allowing them to transmit the virtual currency to a different address [12].

A 51% assault is when an attacker controls more than 51% of the computer power in cryptocurrency networks like Bitcoin, tampering with transaction records and regulations in a blockchain network. Attackers can use this attack technique to carry out harmful operations on network transactions, such as tampering, double spending, and denial of service. Blockchain networks often use consensus procedures like proof-of-work (PoW) or proof-of-stake (PoS) to secure the network.

In a timestamp attack, the attacker modifies the timestamp in the transaction record of a cryptocurrency like Bitcoin to deceive other nodes and perform as double-spending. Attackers frequently double-spend by fiddling with network timestamps or their own computer time to make nodes believe that the transaction comes before other transactions. Cryptocurrency networks generally date transaction records and use consensus techniques to verify the sequence of transaction records to prevent timestamp attacks [13].

(3) Security threats in the application layer

Threats to application-layer security are some security concerns and hazards that could apply to blockchain applications. These dangers can result in attacks on smart contracts, asset theft, compromised private keys, unauthorized access, and other problems. The two most significant application-layer security risks are weak smart contract security and unauthorized access.

Smart contracts are an important part of a blockchain application, and their security is critical to the security of the entire application. However, due to the negligence or accident of the programmer, vulnerabilities may be introduced in the smart contract, resulting in attackers obtaining sensitive information in the smart contract or performing illegal operations through the vulnerability. There are many types of smart contract vulnerabilities, such as integer overflows, re-entrance attacks, logic vulnerabilities, etc. Smart contract exploits can be represented as:

$$S(C) \xrightarrow{call} S'(C) \tag{2}$$

where $S(C)$ is the contract state, $S'(C)$ is the updated contract state, and $\xrightarrow{call}$ represents the function call operation initiated by the attacker. A re-entrance attack is when an attacker exploits a vulnerability in a contract to call another contract when calling another contract, thereby performing malicious actions in the attacker's contract, such as stealing assets.

Therefore, to avoid these vulnerabilities, developers need to adhere to contract writing best practices and conduct comprehensive security tests to ensure the security of smart contracts [14]. Illegal blockchain app access is another security risk. Criminals hack blockchain apps via brute-forcing passwords, social engineering, or other means. In a Bitcoin exchange, an attacker could employ social

engineering to get a user's login credentials and steal assets. To safeguard users' identities and assets, blockchain apps need multi-factor authentication and stringent password regulations [15].

(4) Other kinds of security threats

Exploiting flaws in encryption algorithms or their implementations constitutes a form of threat known as an attack on an encryption algorithm. These assaults can take the form of side-channel attacks, which take advantage of flaws in the physical implementation of the encryption method, such as power consumption or electromagnetic radiation, or brute-force attacks, which require attempting every key until the proper one is discovered.

On the other side, reentrancy attacks are a kind of flaw that can appear in smart contracts or other kinds of software that permit reentrant calls. In this kind of attack, a function is repeatedly called by the attacker before the preceding invocation has finished.

2.2 Threat Assessment Process

Blockchain technology's security is a crucial component in assuring its dependability and trustworthiness [16–18]. Security risks in the blockchain typically fall into one of three categories: network layer, protocol layer, or application layer. The dangers can be examined by doing the following steps:

- Establish the assessment's scope and goals. The assessment's scope might range from the entire blockchain system to a single node, contract, or application. The assessment's goals, such as identifying and averting potential threats and vulnerabilities, must be obvious at the same time.
- Get data and information: gather pertinent data and information about the blockchain system, such as the setup of nodes, the use of protocols, and the source code of applications. It's also necessary to acquire data on prospective risks such known as attack types, security flaws, and malevolent conduct.
- Threat identification: To detect potential threats and vulnerabilities, it is important to examine the information and data that have been gathered. It is important to recognize and evaluate each threat tier separately. For instance, threats at the protocol layer may include double-spend attacks and 51% attacks; threats at the network layer may include DDoS attacks and denial-of-service attacks by nodes; and threats at the application layer may include smart contract vulnerabilities and malicious transactions, among others.
- Determine the significance and propensity of threats: To decide which threats are most important and need to be addressed first, consider their impact and likelihood. For instance, a threat should be prioritized if it has the potential to result in a major data breach or corruption.
- Create security policies and measures: Create relevant security policies and measures to reduce or eliminate the impact of threats based on the findings of the assessment. Defensive strategies like raising the number of nodes and establishing decentralized storage can be developed, for instance, in response to potential attack types.
- Install and monitor security measures: Integrate the created security measures and policies into the blockchain system. Afterward, monitor them and make necessary adjustments to maintain their dependability and efficacy. For instance, keep an eye on network traffic and node status in real-time to spot and stop any assaults.

In conclusion, identifying and evaluating threats at various levels and developing matching security policies and procedures are necessary for blockchain security threat assessment. To maintain the security and dependability of the blockchain system, this method must be continuously reviewed and modified.

3 Research Status of Blockchain Defense Technology

3.1 Single Node Defense Technology

The most popular method of blockchain protection is deployment defense on a different node. The term "single-node independent defense" refers to a single node defending itself using its defense mechanisms, primarily using cryptography, encryption, hashing, digital signature, authentication, and key management technologies. The advantage of this strategy is that the defense technology established on a single node can be ported to other nodes and is extremely portable. The security guarantee of this method primarily depends on the security of the single node itself. The single-node defensive technology is discussed in this section along with its current state of development and area of concentration.

Cryptography can offer significant protections for the confidentiality, integrity, and availability of data. Cryptography is frequently employed in blockchain technology to ensure security and dependability that safeguards blockchain data and transaction information [19–22].

According to the paper [23], cloud computing can offer greater processing power and storage capacity as well as enhanced data privacy and identity security. It introduces post-quantum cryptography, a development in internet security technology. Similar optimizations may be made for post-quantum cryptography technology, literature, and algorithms [24]. Post-quantum cryptography technology has to be optimized in the context of constrained computation and storage resources, taking into account the resource limitations of Internet of Things (IoT) devices. To increase the security and functionality of IoT devices, post-quantum cryptography is implemented utilizing specialized hardware, enhanced algorithms, and current IoT protocols.

(1) Cryptography

To maintain its secrecy and privacy, data can be encrypted and converted into ciphertext. Blockchain may use cryptography to encrypt transaction data and user identities to protect user privacy and prevent fraud.

Traditional keywords for text must scan the entire blockchain, which is wasteful and may expose personal private information. The paper [25] suggested an attribute-based keyword search technique instead. Blockchains that have been encrypted can be rapidly searched without disclosing any personal data. Users can execute fuzzy matching on search terms locally and upload the matching results to the blockchain, which will be confirmed by smart contracts. Another way is to use a fuzzy search for multiple keywords while still encrypting the data first. The smart contract will search the blockchain based on the uploaded matches and provide links to suitably encrypted data. Users can receive plaintext results that satisfy their search criteria by decrypting this data with the corresponding key [26].

Paper [27] offered a novel blockchain security optimal lightweight cryptography image encryption solution for Industry 4.0 environment for secure image transmission for images, combining the benefits of cryptography and blockchain. Designed to address security concerns in IoT contexts by enhancing encryption efficiency and security. To address the issue of privacy leakage during the image retrieval process, Paper [28] suggested a blockchain-based encrypted image retrieval technique (BEIR). With this plan, the user can locate the encrypted image through a keyword search and decrypt it locally. The image is encrypted and stored on the blockchain. BEIR performs superior in terms of privacy protection and retrieval efficiency. As a result, the system can be used in a wide range of contexts, including video retrieval and medical picture retrieval. The historical cryptographic theory put out by the father of cryptography, Engelbarth, was also visualized by paper [29] using cryptography. A smart

contract on the Ethereum blockchain can be accessed to decrypt the encrypted image that is stored there.

To sum up, it is crucial to secure consumers' privacy while dealing with sensitive material like photos. These articles use encryption to safeguard the image's privacy and make sure that only people with permission can view it. Moreover, encryption keys or encrypted photos are stored and managed using blockchain technology. Decentralization, immutability, and dissemination are qualities of blockchain that can guarantee the security and veracity of encrypted data. To perform encryption and decryption operations in contexts with limited resources, the aforementioned article uses a lightweight encryption method.

A suitable model for deployment to multiple nodes must be trained from the perspective of the encryption model for each node to fulfill its specific role. Fairness, security, and dependability must also be guaranteed during training to increase the model's credibility. A smart contract is utilized to coordinate communication between nodes and guarantee the fairness of the training process, and attribute-based encryption technology is employed to secure the training data [30].

The possible weaknesses of single-node defense technology are one area that may benefit from more research. Although this method enables mobility and independence between nodes, it also exposes the entire blockchain network to risk if one node's security is breached.

(2) Hashing algorithm

A technique for converting arbitrary-length data to fixed-length digests is the hashing algorithm. Hashing algorithms can be used in blockchain to check for consistency and integrity. A hash value is computed for each block in the blockchain by running all the transaction data contained in that block through a hashing algorithm. When a block is formed, its hash value is broadcast to the whole network so that other nodes can use it to calculate the block's integrity and immutability. For instance, the hashing algorithm in Bitcoin is used to check each block's proof-of-work to make sure it is accurate and consistent.

As blockchain technology advances, an increasing number of transactions will be recorded on the blockchain. Hence, to handle the increasing amount of data, hashing algorithms must be faster and more efficient, and how to solve the efficiency of hashing algorithms is a hot subject. Parallel Residue Carry Adder-based hash algorithm optimization is suggested, and Field Program Gate Array (FPGA) is used to construct the algorithm [31]. According to experimental findings, the suggested hashing algorithm performs better and uses less space than other standard hashing algorithms, which can increase the performance and efficiency of blockchain applications.

Paper [32] investigated how cryptographic hashing algorithms and Elliptic Curve Secret Sharing (ECIES) can be utilized to improve the security of blockchain in cloud computing and IoT contexts. The authors carry out experimental experiments and provide a cryptographic strategy based on ECIES and the hashing algorithm. The system makes use of ECIES to safeguard both private and public keys as well as a hashing algorithm to ensure that all transactions are legitimate. Experimental findings demonstrate that the plan can enhance blockchain's capacity for privacy and security protection. Paper [33] presented a hashing algorithm implementation technique for the RISC-V processor and a memory computing technology based on Memristors. Verilog Hardware Design Language (HDL) was used by the authors to design and build the method, and an FPGA platform was used for simulation. The technique can increase the speed and effectiveness of hashing algorithms and give improved performance and endurance for blockchain applications, according to experimental data. The hashing

algorithm's computation speed is greatly increased by the employment of the RISC-V processor and Memristor as the memory unit, respectively, in the scheme.

Blockchain technology could incorporate quantum-resistant hashing techniques. Quantum computing may make hashing methods vulnerable to brute-force attacks. Thus, investigating quantum-resistant hashing algorithms could boost blockchain network security. Blockchain hashing algorithms use energy. Hashing algorithms' energy use is an issue because blockchain mining and verification need a lot of processing power. Energy-efficient hashing algorithms and blockchain protocols could make blockchain technology more sustainable. Hashing methods and blockchain network interoperability may also be interesting to study. Sharing data and transactions between specialized blockchain networks will become increasingly vital. Standardized hashing algorithms that enable blockchain network interoperability could boost blockchain adoption and efficiency.

(3) Digital signature

Digital signatures validate digital documents. Blockchain technology lets digital signatures validate transactions, prevent fraud, and avoid double-spending. Digital signatures reveal who originated a transaction and whether its information was changed. Digital signatures can verify user identities to prevent impersonation and identity fraud. Digital signatures use asymmetric cryptography's public and private keys. Digital signatures are created by hashing the original material and encrypting it with the private key. The recipient verifies the digital signature's accuracy with the public key. A blockchain participant's private key can be used to digitally sign transactions, and other nodes can use the public key to verify those transactions. Digital signatures prevent blockchain attacks like altering and forging transactions.

Academics have focused on ensuring transaction legitimacy and integrity while minimizing time and expense in recent years. A quantum-resistant digital signature blockchain system is proposed. The authors use the Hash-based Signature Scheme to compare XMSS and SPHINCS+ quantum-secure digital signature algorithms. Experiments prove the scheme works [34]. A distributed, low-power wide-area network (LPWAN) architecture that uses digital signature and blockchain technology to control devices, process data, and transfer money [35]. The authors suggest a brand-new consensus algorithm that could increase the system's scalability and security. To guarantee the legality of the device, the authors additionally present a physical device-based authentication system. A blockchain transaction security system based on quantum technology is suggested in the paper [36]. Digital signatures are implemented via quantum state transmission and quantum random number generation, and quantum key distribution is used to ensure the security of the keys. The authors suggest a quantum state transmission-based blockchain inter-node communication protocol, which can increase the system's security and dependability. A novel two-parameter elliptic curve digital signature algorithm was suggested in the paper [37] to increase the speed and security of blockchain transactions. The authors evaluate the performance of current digital signature algorithms and suggest a more efficient technique that can save time and space. Via trials, the authors confirm the algorithm's viability and effectiveness. A blockchain- and linear elliptic curve-based cloud server security approach was suggested in the paper [38]. The authors suggest a new elliptic curve-based digital signature algorithm that could increase security and productivity. A blockchain-based authentication system that shields cloud servers from harmful attacks is also introduced by the authors.

(4) Authentication

A technique for verifying a user's identity is authentication. By confirming a user's legitimacy and identity using their public and private keys, blockchain authentication can be accomplished. Blockchain authentication is a crucial security issue that necessitates the creation of more dependable

and secure technologies and solutions to safeguard users' digital assets and private data. Blockchain authentication is a crucial security issue that necessitates the creation of more dependable and secure technologies and solutions to safeguard users' digital assets and private data. Hackers will be able to perform transactions and access digital assets using the user's identity if they can get hold of the user's private key, which might result in significant financial losses and security difficulties.

There are numerous application cases and various implementation techniques to consider when exploring blockchain authentication algorithms. The paper [39] suggested a certificate certification system based on blockchain technology to address the issue of current certificate certification in Vietnam. The system store and verify certificates on the blockchain using smart contracts and encryption, guaranteeing their authenticity and immutability. The system can increase the efficiency and security of certificate authentication in this way. The paper [40] suggested a hybrid blockchain-based identity authentication system for the safe communication of several wireless sensor networks (WSNs). The plan integrates blockchain technology with conventional encryption methods to increase communication security and identity identification. For fog computing settings, the paper [41] suggested a secure authentication system based on blockchain technology. The system uses cryptography and smart contracts to enhance authentication efficiency and protect user identity and personal data. The approach can boost authentication's effectiveness and security in this way. The paper [42] suggested a blockchain-based anonymous identity authentication system for use in edge computing environments. The system makes use of multi-party secure computing technology, zero-knowledge proof technology, and blockchain technology to store and verify user identification information as well as anonymous identity authentication. The plan enhances authentication security and privacy while safeguarding user data security in this way. To increase the security of identity verification, the paper [43] also suggested a multi-factor authentication system based on decentralized identification (DID) and random terminal selection. The system employs blockchain technology to store and validate user identification data and employs a variety of randomly chosen authentication techniques to guarantee security. The approach can boost authentication's effectiveness and security in this way. The paper [44] recommended a transaction authentication method based on blockchain that is resistant to quantum attacks. This method combines conventional and quantum encryption to boost security. This strategy can improve transaction authentication security and offer a robust barrier against attacks by quantum computers.

(5) Key management

Passwords and encryption keys may be safely managed via key management. A user's private key may be safely stored using key management in blockchain to stop private key leakage and theft. Blockchain technology is being used by academics to improve already available solutions or develop new ones that will meet specific security, privacy, and efficiency challenges.

The paper [45] examined the application of blockchain technology in supply chain management and discusses its potential role and benefits for enhancing transparency and traceability, preserving security, and boosting efficiency. It also discusses how blockchain technology can be used to enhance the key goals of supply chain management. To ensure the privacy, accuracy, and accessibility of sensitive data in mobile edge computing, the paper [46] suggested a secure blockchain technology key management system. Using mobile edge computing and blockchain technology together suggests a key-based access control approach that can safeguard sensitive data in mobile devices. The purpose of this paper is to solve security issues in mobile edge computing by offering a secure key management system. To increase the security and privacy of IoT devices, the paper [47] investigated how blockchain technology might be utilized to strengthen key management procedures in Low Power Wide Area

Networks (LoRaWAN). Using permission control methods, integrating blockchain technology into LoRaWAN's key management procedure, and ensuring a secure connection between IoT devices. The goal of this article is to safeguard IoT device communication over LoRaWAN by offering a trustworthy and secure key management solution.

To safeguard secure communication between IoT devices and intelligent transportation systems, new key management strategies based on blockchain technology have also been developed. A blockchain-based threshold key management system is suggested to enable safe and effective communication between automobiles and infrastructure. To secure communication in the blockchain-based intelligent transportation system, a threshold key management technique is presented. This article has the impact of improving the security and effectiveness of intelligent transportation systems by offering a trustworthy key management scheme to safeguard the connection between cars and infrastructure [48]. To protect the secrecy and integrity of data flow across various heterogeneous intelligent transportation systems, paper [49] suggested a dynamic blockchain technology key management system. It is suggested to use a dynamic key management system based on blockchain technology to make data interchange for intelligent transportation systems safer and more effective. This work addresses the security issues of data sharing between diverse intelligent transportation systems by offering a safe and effective key management strategy.

Future developments in supply chain management, mobile edge computing, low-power WAN gear, intelligent transportation systems, and other areas will all depend more and more on blockchain technology. Systems for managing keys on the blockchain can increase security, privacy, openness, and effectiveness. Blockchain technology will become a key tool for ensuring the security and integrity of data transmission in these systems as the demand for intelligent and secure data exchange rises.

3.2 Collaborative Defense Technology

Multi-node collaborative defense technology creates a distributed defense network to improve blockchain defense. In particular, multi-node collaborative defense technology uses the blockchain's decentralized and immutable qualities to identify and protect against various attacks. Multi-node collaborative defense technique reduces network attack system impact by improving defensive capabilities and reaction times.

Multi-node collaborative defense involves multiple nodes working together to secure the blockchain system. Each node in a multi-node collaborative defense can defend itself, but they must work together to produce a stronger defense system. This method's security relies on system coordination and node security. Coordinated and verified nodes can detect and exclude compromised or attacked nodes to protect system security.

Thus, security distinguishes blockchain's single-node independent defense from the multi-node collaborative defense. The single-node independent defense relies on node security, while multi-node collaborative defense requires coordination and verification. Multi-node collaborative defense is often more secure and reliable than single-node independent defense because it can coordinate and verify between nodes. The schematic diagram of the multi-node collaborative defense model is shown in Fig. 2.

Conventional distributed denial-of-service (DDoS) security mechanisms are insufficient to thwart widespread assaults. As a result, combining defensive strategies has shown to be a desirable alternative to raising individual systems' defense capacities. Hardware and software capabilities are frequently lacking in traditional centralized protection strategies. On top of the current distributed architecture, defensive services are offered through a cooperative, multi-domain DDoS mitigation system [50].

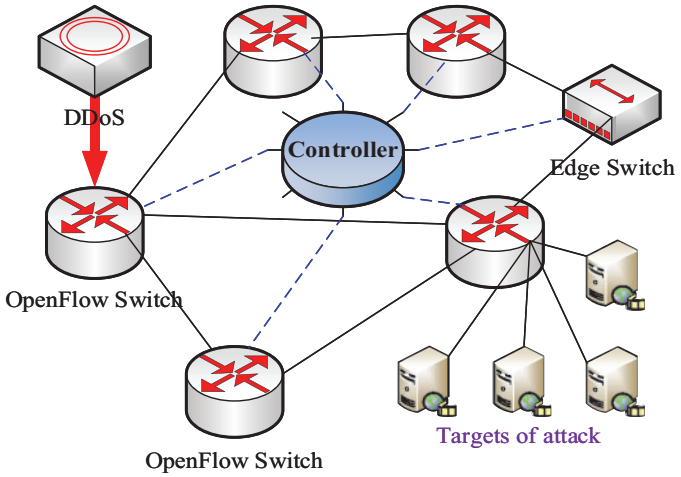

Figure 2: The schematic diagram of the multi-node collaborative defense model

Since the Internet includes several easy-to-use yet powerful attack vectors, such as distributed denial-of-service (DDoS) attacks, cybersecurity has expanded rapidly over the past two decades. Due to the rapid expansion of collaborative environments like the Internet of Things, cloud computing, and software-defined networking, DDoS attackers have many new opportunities to exploit their scattered nature. Attackers can create hordes of bots to conduct huge attacks anonymously by infecting devices. Thus, DDoS prevention must be effective and efficient. The author discusses DDoS threat assessments and cutting-edge security techniques in numerous domains.

Interactive dashboards can display the state of current threat mitigation in a blockchain-based collaborative defense platform, allowing security analysts to respond to attacks at the individual or group level. BloSS is a cooperative, multi-domain DDoS defense system built on the blockchain, where each autonomous system (AS) joins a defensive consortium. While not interactive or visually appealing, BloSS's operational implementation is now automated for DDoS mitigation. A security management dashboard that gives a summary of all attack-related data was created by to enable interactive use by cybersecurity analysts. This dashboard enables human decision-makers, such as security analysts, to assess the seriousness of a threat and determine the best course of action. The operational complexity of blockchain-based cooperative defense is decreased by this actionable governance dashboard. The paper [51] introduced a threat management dashboard that offers cybersecurity experts a straightforward, impartial user interface. You may handle mitigation and service requests from other businesses using the dashboard, and you can follow their development. The study also completes BloSS's first architecture, which is built on a blockchain with proof-of-grant consensus, enabling dashboard-based visualization and management of collaborative defense requests. A collaborative multi-domain DDoS system's participants lack incentives for collaboration and reputation. The reward system can therefore offer the necessary incentives to encourage collaboration between service providers and customers. Paper [52] discussed the development, implementation, and assessment of the Blockchain Signaling System's reputation mechanism (BloSS). Smart contracts' reputation management system reduces bad behavior by rewarding design. Beta reputation data rewards honest players. BloSS fights large-scale DDoS attacks together. The blockchain-based multi-domain cooperative DDoS defense solution lets autonomous systems (ASs) create defensive coalitions and share attack information on Ethereum. BloSS is not interactive or graphic but automates

DDoS mitigation. Human cybersecurity analysts evaluate real-world defense systems for DDoS mitigation. This study delivers an interactive BloSS security management dashboard for cybersecurity experts [53].

With the IoT's quick expansion, network resource growth and security issues have gotten progressively worse. It is vital to figure out how to efficiently combine network resources and improve defense capabilities. Intelligence about cyber threats is essential for carrying out proactive defensive measures. It offers a forum for knowledge exchange that not only improves security preparation and awareness but also enables the defense to lessen the impact of future assaults.

In [54], to make it easier for various players to share information about cyber threats, the authors suggested a distributed security paradigm. The suggested solution makes use of smart contracts and blockchain technology to ensure immutable logic and tamper-proof record keeping. To develop blockchain applications, we leverage Hyperledger Fabric, an open-source blockchain platform. We also incorporate software-defined networking into the suggested shared platform, making use of its adaptability and administration capabilities.

Threat detection and response are destined to fail in the absence of a sound security design framework. The essay tackles topics including traceable mobile smart objects, intruder threat detction, and more while also putting out a framework to help digital forensics and incident response. A federated blockchain concept is also introduced in the paper to provide a digital chain of custody and a teamwork environment to help post-incident investigations. An attacker controls a botnet of infected internet PCs. Decentralized P2P topologies increase attack and defense in modern botnets. Bad actors employ IoT devices to attack, making them crucial in this situation. IoT botnets DDoSed Krebs on Security. Due to zombie devices' regular contact and community formation, AutoBotCatcher is the first step in discovering P2P botnets in the Internet of Things. Thus, AutoBotCatcher dynamically monitors IoT device network traffic to detect botnets. AutoBotCatcher employs a Byzantine Fault Tolerant (BFT) blockchain as a state transition machine to enable collaboration and dynamic botnet detection by collecting and monitoring IoT device network traffic. To better understand AutoBotCatcher's architecture, this article first defines its underlying blockchain structure before going into each of its parts [55]. In [56], a platform for cooperative distributed denial-of-service (DDoS) attack mitigation built on blockchain is called Co-IoT. To enable attack collaboration between domains based on software-defined networks (SDNs) and to convey attack information in a safe, effective, and decentralized way, the framework makes use of smart contracts, namely Ethereum smart contracts. In Ropsten, the official Ethereum Testnet, Co-IoT is being implemented. According to experimental findings, Co-IoT is flexible, effective, secure, and cost-efficient, making it a potential countermeasure to massive DDoS assaults. Future smart city security will have new chances thanks to Co-IoT as the Internet of Things expands.

To establish cooperative defensive mechanisms amongst businesses and lessen the effects of DDoS assaults on legitimate users, the paper [57] offered a framework called shieldSDN and shieldCHAIN that leverages P4, SDN, and Blockchain technology. By removing attack indications and transmitting them to other companies so they can successfully defend against the same botnet assault, the system allows packet filter synchronization between several organizations. Via four experiments—the first of which is carried out within the organization, the second, third, and fourth of which are carried out throughout the organization—the framework confirms the viability of its intended purpose. The framework offers community members the chance to work together and defend against botnet DDoS assaults since it is the first solution to incorporate P4 switches, SDN controllers, and Blockchain technology for such use cases.

The paper [58] introduced SC-FLARE, a smart contract collaborative signaling system for completely distributed and automated attack information sharing, incentive exchange, and reputation tracking. SC-FLARE is built on the Ethereum proof-of-authority blockchain. SC-FLARE offers the collaborative platform required to execute collaborative defenses without the need to manage, construct, and develop specific registries and gossip protocols by utilizing blockchain and smart contracts. DDoS assaults are still one of the top worries for service providers all around the world. Trusted computing and blockchain, which are developing technologies for information security protection, may provide a secure and dependable operating environment and management system for the power Internet of Things. This paper [59] built a distributed decision-making and collaborative autonomous model based on blockchain with the aid of the thorough evaluation algorithm of fuzzy mathematical set theory, establishes a security protection model of "manageable and controllable, precise protection, visible trustworthiness, and intelligent defense," performs trusted computing and privacy protection for computer blockchain IoT nodes, and substantially improves the information security.

Dynamic topic modeling and network analysis will examine Korean blockchain research trends. Paper [60] used collaborative network analysis between universities and research institutes, keyword co-occurrence network analysis, and time series topic analysis. We found Soongsil University, Soonchunhyang University, Korea University, KAIST, and major research institutes like the Ministry of Defense, Korea Railway Research Institute, Samil PricewaterhouseCoopers, Electronics and Communications Research Institute, and others through a network analysis of university-research institute collaborations. Next, keyword co-discovery network analysis revealed the major study keywords: virtual assets (cryptocurrencies, Bitcoin, Ethereum, virtual currencies), blockchain technology (distributed ledger), finance (smart contracts), and information security (security, privacy, personal information). Smart contracts have the greatest network centrality score. Eventually, time series topic analysis revealed five primary themes: blockchain technology, blockchain ecosystem, blockchain applications 1 (trading, online voting, real estate), blockchain applications 2 (food, tourism, distribution, media), and blockchain applications 3 (economics, finance). Examining each subject's representative keywords also reveals topic changes. This study is the first to use time-series subject analysis, university-research institution collaboration network analysis, and dynamic topic modeling to examine Korean blockchain research trends.

Collaborative Intrusion Detection System (CIDS) nodes provide important detection-control information for collaborative defense. Software-defined networking (SDN) provides network controllers for multi-autonomous system networks, making it a key platform for CIDS applications. CIDS research still lacks the robust trust management and collaborative defense integrity protection of SDN controllers to defend against insider attacks and avoid transmitting untrue and malicious detection signatures to other participating controllers.

According to the paper [61], satellite internet (SI) will dominate 6G and outperform terrestrial Internet. Due to limited processing power and bandwidth, distributed denial-of-service (DDoS) attacks can damage SIs or bring down networks. The current DDoS prevention technology requires a lot of computational power and bandwidth, making SI use problematic. A blockchain-based distributed collaborative ingress defense (DCED) architecture that captures and aggregates network traffic at SI ingress can protect SIs from DDoS attacks. Ingress control, digest virtual aggregation, and distributed detection digest handlers make up the framework. The earlier application recognizes, extracts, and pushes DDoS multidimensional signatures into the blockchain. Later systems aggregate attack signatures from block data, compare them to a baseline, and notify users using MapReduce. Policies full traffic filtering. The IXIA platform creates malicious traffic in trials, and the framework

can swiftly and consistently identify attack traffic with an area under the receiver operating characteristic curve of 0.99 in 1500 milliseconds. The proposed DDoS method protects SI bandwidth resources more than comparable methods.

A collaborative model of simultaneous distributed learning is built utilizing shared memory across numerous computing devices, which is motivated by the benefits of the decentralized method, using blockchain smart contracts as a security incentive mechanism. In terms of increasing user privacy, this collaborative approach keeps the dispersed learning value drive. It enables a blockchain-based safe decentralized incentive system with zero single points of failure. In addition, possible weaknesses and countermeasures are described. The collaborative model was strongly advised by the experimental findings for achieving the design objectives [62].

In terms of resources, different scholars have used different means to improve this problem.

Worm computing, a decentralized platform inspired by benign network worms, was proposed in the paper [63]. Worm computing, which gathers data for resource sharing and cooperative defense, boosts resource utilization, computing capacity, and network security. Data sharing and trust computing in the standard collaboration paradigm are solved, and decentralized and trusted services assure transaction immutability. Private chains contain collaborative data on the blockchain network. The authors examine resource consumption and cooperative defense against malicious URLs, and the worm computing paradigm maximizes resource use and network security.

SDN increases network flexibility and programmability by separating the control and data planes. Logically centralized control makes the control plane vulnerable. A hostile third party can employ reactive forwarding to DDoS the SDN controller. However, without collaborative detection and prevention approaches, standard single-controller DoS/DDoS solutions fail in multi-controller scenarios. We recommend BSD-Guard, a blockchain-based SDN Targeted DDoS defense Framework. Our framework can identify and defend SDN controllers cooperatively. BSD-Guard adds a secure blockchain-based intermediate plane between the control and data planes. The security intermediate layer evaluates the suspicious rate of new traffic and transmits the suspect list to the blockchain for immutable storage and distribution based on packet data. Pre-deployed blockchain smart contracts are a cooperative defensive approach based on SDN domain suspicious list reports. The security intermediate plane turns defense policies into flow table operations and installs them into switches. Experimental results show that BSD-Guard can accurately determine the attack path and identify DoS/DDoS attacks under many controllers [64].

By monitoring and exchanging data across several industries, Cyber Threat Intelligence (CTI) technology is an evidence-based security system that proactively handles information concerning sophisticated cyber threats. The creation and spread of ineffective protection techniques can have a substantial impact on the effectiveness of CTI systems. In this study, a novel collaborative cyber threat information exchange (CCTI) system based on blockchain artificial intelligence computing material is proposed, highlighting the capacity of a larger group to assist in identifying vulnerabilities [65].

Cyber Threat Intelligence (CTI) is an evidence-based security system that monitors and exchanges information across industries to proactively handle sophisticated cyber threats. Poor protection techniques might reduce CTI system efficiency. This study offers a blockchain AI-based collaborative cyber threat information exchange (CCTI) system that emphasizes larger group vulnerability identification [66].

Federated learning is already making its mark in this field.

Using federated learning (FL), several linked devices may create deep learning models while retaining their training data locally. FL transmits a local gradient progressively instead of sending the training data and model to the server. Thus FL ensures data privacy from the beginning. FL uses a decentralized strategy and stops centralizing training data. Similarly to this, blockchain follows the same methodology and offers a digital ledger that can make up for the drawbacks of centralized systems.

The response of network providers to distributed denial-of-service attacks was examined in [67]. They can handle the onslaught or divert traffic to another shuffling center. If manufacturers chose the former, distributed security systems are the best way to prevent this assault. This paper proposes a federal network that uses blockchain technology for signaling, coordination, and orchestration to eliminate hazardous traffic in linked and disconnected autonomous systems (AS). Mitigation history determines AS reputation scores. Combinatorial optimization weights network traffic and reputation scores to distribute defense resources among numerous partners. Malicious traffic is decreased inside the eXpress Data Path (XDP) architecture using a configurable network data channel, allowing operators enhanced packet processing throughput and cutting-edge filtering flexibility. A proof-of-concept prototype and real network evaluation tested our method.

Researchers at Sun Yat-sen University proposed the distributed and autonomous federated learning framework BFLC (blockchain-based federated learning framework with committee consensus) based on blockchain systems to address performance issues in decentralized systems, particularly security issues, in 2020. To demonstrate the security of the framework, the training procedure and the committee consensus mechanism maximize the consensus effectiveness and storage consumption [68].

In 2020, the security framework of federated learning is proposed to use the capabilities of blockchain smart contracts to resist poisoning attacks and introduce localized differential privacy technology to resist member inference attacks. This is done to counter the two threats of poisoning attacks and member inference attacks in federated learning under 5G networks [69]. Similar research has been used in crowdsourced IoT, where paper [70] employed differential privacy strategies to guard against assaults by bad actors leveraging blockchain to record crowdsourcing actions to deduce sensitive personal information while undertaking federated learning.

Blockchain-based federated learning for fog computing was suggested in the paper [71]. They make use of distributed hash tables to improve data storage on the blockchain, enhancing block production efficiency, combining distributed privacy protection with the benefits of blockchain decentralization, and resolving the single-point failure issue in fog computing situations. Moreover, the issue of poisoning attacks in federated learning is resolved by eliminating the central server.

In paper [72], a set of blockchain-based federated learning frameworks called BlockFL were proposed to address the scenario of local model updating on mobile devices. By connecting mobile devices, miners enable users to earn money by trading their local models, while miners exchange and verify all local models and then carry out proof-of-work to earn money. The global model update is unaffected by the failure of a single miner or device, which further increases the system's resiliency.

In 2019, paper [73] presented a new federated learning architecture to increase the effectiveness and security of data sharing and introduces permission chain and directed acyclic graph (DAG) technology for the Internet of Vehicles scenario. An asynchronous federated learning method is suggested as deep reinforcement learning is also used for node selection to boost performance. The literature-proposed FLchain [74] proposed the idea of a channel in the blockchain to train different global models, get the chosen global model through consensus, and save the local model parameters as a block in a particular ledger. In contrast to the conventional federated learning model, the author suggests the idea of a global model state tree, which resolves the model's global parameters by the consensus of the state tree.

Different application fields need to achieve collaborative defense for different practical needs, and the combination of technology in professional fields is also a research hotspot.

This type of interdisciplinary and multi-field cross-research can solve unique problems in a targeted manner, and it can be well applied to the scene after targeted analysis has been performed on it. Unique models and defense measures can be established for various application fields according to the particular characteristics of the field.

Paper [75] described a system of wind energy. Wind energy is expanding, but frozen blades are an issue. The data-driven technique detects leaf icing, but it collects a lot of IoT data to a central server, which might leak valuable company data. BLADE, a blockchain-enhanced imbalanced federated learning (FL) model for leaf icing detection, addresses this problem. Blockchain improves privacy, the FL model, and server failure. Block harmful assaults via a blockchain verification system. BLADE also solves sensor data category imbalance using a new imbalance learning algorithm. Two wind farms tested 10 BLADE wind turbines. Experimental findings demonstrate BLADE's efficacy, superiority, and practicality.

Paper [76] described a vehicle in the growing number of network devices and software expansion and wireless interfaces, the Internet of Vehicles risks network penetration. A cooperative intrusion detection system based on distributed edge devices (such as linked automobiles and road edge units (RSUs)) offloads the training model to distributed edge devices, reducing central server resource consumption and ensuring security and privacy. Blockchain secures trained models. This study investigates typical threats and indicates that the suggested system reduces communication overhead and processing costs to defend vehicle privacy cooperatively. The distributed federated learning technology increases intrusion detection system efficiency and protection while guaranteeing security and privacy.

There are also applications in medical science [77], digital genome-based device integrity checking to identify network attacks. Digital genomes are based on medical genomes, which calculate the integrity of critical hardware, software, and other device components. Hence, if an attacker alters a node's hardware or software, the digital genome will change, making it easier to identify. The technique ensures end device legitimacy and enables security and performance analysis in IoT and other IT applications. Cooperation intrusion detection systems protect against many network assaults, but if an inside attacker compromises nodes, it can harm the entire collaborative network. Hence, network attackers must be identified and stopped.

Also, applications for traditional network issues like IPV4, IPV6, etc., [78]. IPv6, which addresses IPv4 address depletion, requires the usage of ICMPv6 packets to leverage new capabilities like Neighbor Discovery Protocol (NDP). This worsens ICMPv6-based DoS and DDoS assaults. For ICMPv6 DoS and DDoS assaults, researchers suggest anomaly-based and signature-based intrusion detection systems (IDS). Yet, without a more complete understanding of machine learning (ML) methods, classifiers, feature selection approaches, datasets, and assessment measures, the whole picture

of IDS with ML techniques is difficult to discern. This research classifies ML-based IDS to identify ICMPv6-based DoS and DDoS threats and presents a way to distinguish between single and hybrid classifiers. The ensemble framework also suggests using blockchain in collaborative IDS (CIDS) architecture to solve ICMPv6 DoS and DDoS attack detection difficulties. This article classifies DoS and DDoS attacks by ICMPv6 vulnerabilities for future researchers. This is the first review article on ML-based IDS, and it presents ensemble learning-based IDS models to attract academics.

Blockchain and Artificial Intelligence (AI) in joint defense systems could be a study topic. Future research may benefit from studying how these technologies might be combined to produce more powerful defense systems. In medical science, joint defense systems have ethical considerations. Digital genomes and IoT are used for security and performance analysis, thus personal data and privacy must be secured and dangers and vulnerabilities acknowledged and handled. Thus, investigating ethical frameworks for collaborative defense systems in many application sectors could assist ensure their responsible development and use. It also emphasizes interdisciplinary and multi-field cross-research for focused problem-solving. This shows that computer science, engineering, and medical science experts working together could accelerate joint defense system development and implementation.

We suppose to develop a blockchain-based voting tool, named SecureVote, which promises secure, transparent, and decentralized voting. SecureVote lets voters utilize the blockchain to vote and verify the results using a consensus mechanism, assuring fairness and legitimacy. We can address the following collaborative defense issues by implementing this system: (1) Authentication: SecureVote voters must be authenticated before voting. This authentication mechanism must be secure and dependable. Attackers could rig elections with phony identities. Strengthening identity verification can improve voter identification accuracy. (2) Voter privacy: The blockchain is public, thus others can see voters' votes. Thus, voting results must be kept confidential and only viewed by authorized people. Encrypting voting results and restricting access to them solves it. (3) 51% assault: A blockchain node with over 51% processing power can maliciously attack the blockchain. In SecureVote, an attacker with most of the hash power can change vote results or reject service. (4) Smart contract vulnerabilities: SecureVote manages voting through smart contracts, which can be vulnerable to 51% assaults. Attackers may use smart contract flaws to launch reentrancy attacks, etc. A smart contract security audit solves it.

Researchers have developed new computer system efficiency and security solutions. In the framework of current computer science breakthroughs, emerging technologies like artificial intelligence and blockchain will become increasingly relevant in future studies.

These studies show that computer systems are more insecure and inefficient, but they also provide fresh solutions and insights for future studies. These findings also demonstrate that emerging technologies like artificial intelligence and blockchain will become increasingly significant in computer science research, and more specialists and researchers are needed to help advance the area.

4 Research on Blockchain Security Assessment Methods

4.1 Security Assessment Metrics

The Blockchain security assessment is a process whose purpose is to assess the security of a blockchain system to ensure the security and reliability of the system [79]. The blockchain security assessment should include the following aspects: Data integrity: ensure that the data in the blockchain system is complete and consistent to prevent data from being tampered with [80]; Node security: Evaluate the node security of the blockchain system to ensure that nodes will not be attacked

or hijacked [81]; Data privacy: evaluate the data privacy protection mechanism of the blockchain system to ensure that sensitive data is not leaked [82]; Consensus mechanism: evaluate the consensus mechanism of the blockchain system to ensure that the system can effectively confirm and verify transactions [83]; Smart contract security: Evaluate the smart contract security of the blockchain system to ensure that smart contracts cannot be attacked or hijacked [84].

(1) Blockchain data integrity

- A blockchain's size is measured in bytes and indicates the total quantity of data that is kept on the blockchain. The performance of the node might be impacted if the blockchain is too big.
- The number of blocks on the blockchain is referred to as the blockchain's length. The length may be used to gauge the blockchain's integrity because altered data might shorten the chain's lifespan.
- Hash rate, or the quantity of hashes on each block, is the third factor. Data integrity on the blockchain can be verified using hashes, hence the greater the hash rate, the more trustworthy the data integrity.
- A data integrity check, or DIC, is the procedure of verifying the accuracy of data on a blockchain. For instance, Merkle trees may be used to check the accuracy of vast volumes of data on a blockchain, a distributed data structure. If data integrity problems are discovered, the proper steps can be taken to resolve them.

(2) Node Security

- The number of nodes that are a member of the blockchain network is meaningful. The more nodes there are, the more secure the blockchain network is since it takes more nodes under an attacker's control to impact the entire network.
- The ratio of inbound to outgoing traffic describes how much data a node receives and sends. Stronger node defense is required since a large traffic proportion increases the likelihood that the node will be attacked.
- Network topology: This term describes how nodes are connected in a blockchain network. Complex network typologies increase network security since it takes more work for an attacker to harm the whole network as a whole.
- Node authentication is the procedure used to verify a node's identification. By preventing rogue nodes from joining the network, rigorous node authentication may keep the network safe.
- The separation of several nodes in a blockchain network is referred to as node isolation. When a node is isolated, it indicates that it will not have an impact on other nodes, preserving the network's overall security. If a node fails or is attacked, just that node is impacted by node isolation, not the whole network. Node isolation is thus a crucial safeguard for the security of blockchain networks.

(3) Data Privacy

- Choosing an encryption method is one of the most important aspects of protecting data privacy since it directly impacts the security of the data. Several aspects, including the algorithm's security, accessibility, and effectiveness, must be taken into account while selecting the best encryption algorithm.
- Key length: Key length is another crucial element that affects how secure an encryption technique is. The encryption algorithm is often safer the longer the key is.

- Data privacy is ensured by the security evaluation of encryption methods, which is a crucial step. Several variables, including the algorithm's dependability, stability, and availability, should be taken into account while evaluating security.
- Symmetric/asymmetric encryption: There are two different types of encryption: symmetric encryption uses the same key to encrypt and decode data, whereas asymmetric encryption uses different keys. The sensitivity and security requirements of your data will determine whatever encryption method you use.
- Data deletion policy: When discussing how data is treated to preserve its privacy once it is no longer required, a data deletion policy is used. Securely destroy data to assure that it cannot be retrieved and to stop unauthorized access.

(4) Consensus mechanism

- Selecting the appropriate consensus algorithm is crucial since it will have a direct impact on the system's effectiveness, security, and scalability. Proof of Work (PoW), Proof of Stake (PoS), and Proof of Delegation are common consensus techniques (DPoS).
- Algorithm security assessment: It is crucial to analyze the security of consensus algorithms to make sure that the system's data is not altered and misused. The algorithm's resistance to different assaults and its fault tolerance should both be included in the security evaluation.
- Algorithm performance: The throughput and response times of the system are directly impacted by the consensus algorithm's performance. To guarantee that the system performs well, pick the appropriate consensus algorithm.
- Scalability of algorithms: As the system's size grows, consensus methods' capacity to scale is also essential. The algorithm must be scalable to meet system requirements.
- Node distribution: The security and dependability of the system are directly impacted by the consensus mechanism's node distribution. To avoid single points of failure and assaults in a distributed system, the distribution of nodes should be as even and balanced as feasible. Node distribution also has a direct impact on the system's failure tolerance and rate of data synchronization.

(5) Smart contract security

- A thorough evaluation of the contract code is necessary to make sure that it is free of security risks and vulnerabilities.
- Contract security assessment: Smart contracts' security has to be assessed to make sure that they can fend off different distributed system threats.
- Contract execution efficiency: A smart contract's resource use and speed of execution are referred to as its execution efficiency. The execution efficiency of smart contracts should be as high as feasible to guarantee the distributed system's efficiency.
- Programming language of the contract: To make it simple for developers to write and review code, the contract's programming language should be clear and understandable.
- Contract fault tolerance: A smart contract's fault tolerance is its capacity to maintain the stability and dependability of the system in the case of a breakdown.

Thus, security metrics matter more when applying blockchain technology to IoT, fog computing, and WSN security. A variety of metrics can assist safeguard and preserve data delivered and stored in these systems. IoT systems need authentication, authorization, encryption, availability, privacy, and patch management. These metrics ensure that users are properly identified and authorized to access the system, data is sent securely and privately, and vulnerabilities are rapidly patched. Data

protection, access control, audibility resource utilization, and secure communication become critical in fog computing systems. These metrics assist protect sensitive data, restricting user access, auditing system activity, and securing communications channels. WSN systems need confidentiality, integrity, availability, resilience, survivability, and energy efficiency. These metrics ensure that the system can transmit secret data, detect and prevent unauthorized access or manipulation, remain operational and available despite disruptions, recover from failures rapidly, and optimize energy usage to extend system life [26].

4.2 Research on Safety Assessment Methods

(1) Model-based evaluation methods

Model-based assessment is the process of assessing a system through the construction of an abstract model. By characterizing the structure and behavior of a system, this technique can forecast its performance and safety in certain circumstances. It is feasible to evaluate the system's security and find its security weaknesses by looking at the model the system created. For instance, if you want to assess the security of an encryption scheme, you may create a model that explains how it operates and then use simulation or emulation techniques to forecast its security in various scenarios. The security and effectiveness of the encryption method may be assessed by the study and experimentation of the model [85].

Paper [86] proposed a novel and efficient framework based on model-driven architecture, in particular, defining a metamodel (M2-level Ecore model) that includes the concept of blockchain technology. Paper [87] considers blockchain performance from the perspective of model prediction and benchmarking, presents the results of research on smart contracts in the Ethereum blockchain, and discusses the requirements for a common benchmark of blockchain performance. Paper [88] studies static and transient performance characteristics by combining analytical calculations and simulation experiments. It demonstrates close agreement with the measurements on WAN testbeds running the Ethereum protocol. Paper [89] used a multi-criteria decision-making method to rank and summarize public blockchain platforms. It proposes a new weight assignment technology that combines entropy and CRITIC methods. An important part proposed in the paper [90] is to incorporate graph models into the functionality of the blockchain and its components, while also leveraging its strengths in data analysis by finding relationships between data and extracting their true value.

The advantage of model-based evaluation methods is that they can predict the performance and safety of the system in advance, thereby improving the efficiency and accuracy of evaluation [91]. However, model-based evaluation methods also have some drawbacks, such as the accuracy of the model may be affected by bias and error, which can lead to inaccurate evaluation results [92].

(2) Data-based evaluation methods

This approach uses actual system data for security assessment, including log analysis, report analysis, data mining, and so on. By analyzing the data on the operation of the system, it is possible to assess the security of the system and identify its security vulnerabilities [93].

For example, in network security assessment, attack data in the network can be collected to evaluate the effectiveness of the network defense system [94].

Paper [95] proposed a data-driven model that automatically collects data through crawlers to evaluate blockchain from three dimensions: technology, team capability, and community activity. Paper [96] was exploring computer data security based on blockchain technology and analyzes the advantages of computer data security protection and the security of data verification methods.

Paper [97] investigated attacks on blockchains and develops a set of threat indicators to assess the feasibility of monitoring current blockchain frameworks by aggregating log information from relevant blockchain components.

Paper [98] presents an approach to solving one of the security threats by introducing neural networks into the blockchain consensus mechanism. Paper [99] predicted decentralized blockchain security by using the Long Short-Term Memory (LSTM) network, specifically testing whether LSTM-based neural networks can generate beneficial transaction signals for different blockchains. Paper [100] detected blockchain security attacks through machine learning and software-defined networking methods. It discusses anomaly identification methods centered on encoder-decoder prototypes, trained with collective information obtained by observing blockchain behavior.

(3) Simulation-based evaluation method

This method uses simulation technology to simulate the operation of the system, including simulated attacks, simulated vulnerabilities, simulated access, etc. By analyzing the simulation of the operation of the system, you can evaluate the security of the system and identify its security vulnerabilities.

The simulation-based assessment approach simulates a safety system's operational environment and functioning to assess how well it performs. The fundamental concept behind this technique is to create a simulation environment using computer simulation software, then simulate the operation and assaults of the security system within this environment to determine the security system's performance indicators. While creating and building blockchain systems, blockchain simulators aid in the evaluation of the best configuration settings and make sure that important requirements like security, transparency, and tamper resistance are addressed.

Paper [101] discussed the ability of blockchain to provide reliable proof of data origin in cloud computing, presents vulnerabilities in blockchain cloud computing, and simulates block retention (BWH) attacks in blockchain cloud computing while considering different reward mechanisms. A simulation-based blockchain architecture method was proposed to evaluate its impact on specific additional data items by implementing a simulation environment and conducting a series of experiments [102]. In addition, the paper [103] introduced the BlockSim implemented in Python, including three layers: stimulus layer, connection layer, and system layer, focusing on modeling and simulating block creation through a proof-of-work consensus algorithm. Paper [104] introduced a method to apply the existing simulation tool ABSOLUT to evaluate blockchain implementations on embedded devices to account for important variables such as the efficiency of energy consumption and the timeliness of blockchain transactions in IoT scenarios. The goal of the paper [105] is to use existing simulation tools to replicate the simplified blockchain proof-of-work (PoW) protocol and set different parameters and observations, showing that it is feasible and practical to study blockchain networks with different network sizes and protocols using simulation methods. The findings of the paper [106] found that the results obtained based on the model coincide with the actual statistics, and although only the modeling of blockchain-based cryptocurrencies is simulated, the proposed model can be used to represent a wide range of blockchain-based systems. The method in the paper [107] is scalable and efficient in terms of time and computing infrastructure requirements, and the observations derived by its simulator are consistent with the results of the model based on real Bitcoin transaction data.

Thus, we compare and summarize the three main methods in the following Table 2.

Table 2: Comparison of security assessment methods

Defensive measures	Description	Pros	Cons
Model-based evaluation	Uses mathematical models to evaluate the security of a system.	Can accurately identify potential vulnerabilities and weaknesses.	Requires knowledge of mathematical modeling and may not capture all real-world scenarios.
Data-based evaluation	Uses actual system data for security assessment, including log analysis, report analysis, data mining, and so on.	Provides real-world insight into system performance and security issues.	May not capture all potential security issues and may be limited by the quality of data available.
Simulation-based evaluation	Uses simulation technology to simulate the operation of the system, including simulated attacks, simulated vulnerabilities, simulated access, etc.	Can simulate a wide range of scenarios and test potential security issues.	May not accurately represent real-world scenarios and can be limited by the accuracy of the simulation model.

5 Challenges and Future Research Directions

5.1 Interoperability and Sustainability

Blockchain technology has difficulties beyond security. How blockchain networks communicate is a major issue. Other blockchain networks have evolved, each with its own protocols and consensus methods. Blockchain technology is hampered by networks' incapacity to communicate and transact.

Blockchain technology deployment has a sustainability issue. Nowadays, the majority of blockchain networks employ Proof of Work (PoW) and Proof of Stake (PoS) consensus procedures. High transaction costs and environmental problems result from this. Therefore, more sustainable and ecologically friendly consensus mechanisms are needed to ensure the long-term viability of blockchain technology.

To solve these problems, coordinated actions are necessary. To exploit blockchain technology, governments, regulatory bodies, company executives, academics, and other stakeholders must collaborate. Collaboration can help develop interoperability standards, long-lasting consensus procedures, and answers to security issues raised by bad actors. Collaborations can make it simpler to develop blockchain applications that address practical problems and progress technology.

Proof of work (PoW), proof of stake (PoS), delegated PoS (DPoS), practical Byzantine fault tolerance (PBFT), and proof of authority (PoA) are some of the common consensus methods used in blockchain. Table 3 provides a comparison of various algorithms.

Table 3: Comparison of different consensus algorithms

Consensus mechanism	PoW	PoS	DPoS	PBFT	PoAts
Main idea	Computational power determines the addition of block	Stakes in hand determine the chance of adding the block	Voting and stakes of nodes determine the chance of adding a block	Based on the Byzantine fault tolerance approach	Only a set of authorized nodes are able to add blocks
Energy consumption	High	Low	Low	Low	Low
Scalability	Good	Good	Good	Bad	Good
Fault tolerance	50%	50%	50%	33%	50%
Level of centralization	Low	Medium	Medium	High	High
Application	Public	Public	Public	Private	Private

5.2 Parallel Detection

DDoS attacks frequently result in network delays or breakdowns in typical centralized networks since the attack traffic directly overloads the network infrastructure. Because data is distributed across many nodes in blockchain networks, an assault from a single node is unlikely to bring the network to a halt. Yet, distributed denial-of-service attacks (DDoS) can still have a significant negative impact on blockchain networks since the consensus process in a blockchain network necessitates considerable communication between nodes. The results are based on the CIC-DDoS2019 and CAIDA-2007 datasets. Support Vector Machine (SVM) base learners had poor performance and a high False Alarm Rate (FAR). Random Forest (RF) and Gradient Boosting Machine (GBM) have high FAR, but they outperformed SVM base learners. Model-Based Value Expansion (MVE) beat each base learner in classification accuracy and FAR by combining their strengths [108]. Table 4 provides deep-learning methods for the CIC dataset.

Table 4: Deep-learning methods for the CIC dataset

Classifier	Classification accuracy	Recall	Specificity	F-measure	Detection rate	False alarm rate
SVM	92.96%	96.33%	88.85%	93.75%	91.31%	11.14%
RF	98.68%	99.74%	97.38%	98.80%	97.88%	2.61%
GBM	98.98%	99.27%	98.63%	99.08%	98.88%	1.36%
MVE	99.12%	99.35%	98.83%	99.19%	99.04%	1.16%

Parallel DDoS detection technology is a crucial technique for resolving this issue [50]. This technique can identify attack traffic using numerous inspection nodes at once and combine the detection findings to increase detection accuracy and speed [51]. In comparison to conventional single

detection nodes, using multiple detection nodes can make detection more widespread and attack-resistant.

The following procedures must normally be followed to provide simultaneous DDoS detection in a blockchain network:

(1) Use several detection nodes to guarantee that the whole network is covered by detection. These nodes should be dispersed across the network.

(2) Set up the detection method: To ensure that the detection results can be accurately summarized, these nodes should set up the same detection algorithm.

(3) Put together a specific smart contract in the blockchain network to implement detection result aggregation. Smart contracts can gather and combine the detection data from every detection node and then act appropriately in response to them, such as restricting traffic from attack sources.

Technology for parallel DDoS detection offers special benefits for blockchain defense. It can increase detection accuracy and speed as well as the network's defense against threats. In comparison to conventional single detection nodes, using multiple detection nodes can make detection more widespread and attack-resistant. Moreover, the blockchain network's smart contracts may be used to aggregate detection data, increasing the automation and intelligence of defenses.

The following issues and obstacles may affect parallel DDoS detection in the future:

(1) Large-scale attack processing capacity: DDoS assaults are becoming more widespread as a result of the rising number of Internet users and devices. Future network attacks could be more significant, necessitating concurrent DDoS detection systems with more powerful processing and scalability.

(2) Complexity of attack behavior: To get beyond current defenses, attackers are continually updating their attack methods. Future DDoS attacks could include more sophisticated attack techniques including multi-protocol attacks, low-rate attacks, flood attacks, etc., which need more advanced parallel DDoS detection capabilities.

(3) Resource utilization and false positive rate: Simultaneous DDoS detection uses a lot of CPU and memory, among other system resources. Its resource footprint gets worse as networks expand and attackers get more sophisticated. False positive rates are also a worry, particularly in large-scale assaults when they might have a significant negative effect on the network.

(4) Algorithm optimization and intelligence: As machine learning and artificial intelligence technology advance, more intelligent detection algorithms may be used in the future for parallel DDoS detection to increase detection efficiency and accuracy. The efficiency of concurrent DDoS detection needs to be substantially improved, which calls for both hardware and algorithm improvement.

In conclusion, simultaneous DDoS detection will confront increasingly severe difficulties and challenges in the future, necessitating constant innovation and optimization to combat the changing cybersecurity threats.

5.3 Federated Learning

Federated learning is an emerging distributed machine learning technique that protects data privacy by storing data on local devices and using cryptography to communicate and harmonize [69]. Federated learning can be applied to several fields, including the field of blockchain security [70]. In the future, federated learning has the following development trends in blockchain defense:

Improve data privacy and security: Blockchain technology can ensure the security and immutability of data, while federated learning can further improve the privacy and security of data [71]. In the future, federated learning can be applied to the blockchain to further protect the privacy and security of blockchain data.

Strengthening blockchain consensus mechanisms: Federated learning can help improve the efficiency and accuracy of blockchain consensus mechanisms. In the future, federated learning can be applied to blockchain consensus mechanisms to improve the security and performance of blockchains.

Accelerate blockchain application development: Federated learning can help improve the efficiency and quality of blockchain application development. In the future, federated learning can be applied to the development process of blockchain applications to improve the performance and security of applications.

Promote the integration of blockchain and artificial intelligence: As an emerging technology in the field of artificial intelligence, federated learning can promote the integration of blockchain and artificial intelligence. In the future, federated learning can be applied to blockchain to improve the intelligence and application range of blockchain.

Specifically, federated learning includes the following steps:

(1) Select local devices: In federated learning, multiple local devices need to be selected, which have certain data and computing resources and can complete certain machine learning tasks.

(2) Encrypted data communication: To protect the privacy of data on the local device, encryption technology is required to encrypt and decrypt data. During data communication, the communication is secured using encryption technology to prevent data leakage.

(3) Local training: Train the model on the local device and update the model parameters based on local data.

(4) Model aggregation: Upload the model parameters on the local device to the central server for model aggregation. In the process of model aggregation, you can use a variety of aggregation algorithms, such as the weighted average algorithm and gradient average algorithm.

(5) Global model update: Finally get the global model and update the global model to each local device.

Blockchain technology has transformed security, particularly data privacy and decentralized control. Blockchain can improve system security, especially in federated learning, in collaborative defense. Scalability, security, and privacy issues remain. Future research should improve and speed up federated learning algorithms, combine them with other technologies like the Internet of Things, and create new application scenarios. Addressing these difficulties unlocks blockchain's collective defense potential, enabling new data and system protections.

Federated learning should be studied in several important areas to improve its performance and application possibilities. First, federated learning must improve data privacy and communication security of local devices. This may require discovering novel ways to protect sensitive data and secure federated learning systems.

Second, this technology will depend on good federated learning algorithms. Existing algorithms are promising, but they need to converge faster and more efficiently. Future research should focus on developing better algorithms for more complicated learning challenges and speedier convergence.

Thirdly, federated learning must be integrated with blockchain, the Internet of Things, and other new technologies to broaden its use and influence. This will enable new application scenarios and connect federated learning to other AI research.

As local devices multiply, federated learning scalability will become important. Future research should focus on scalable federated learning systems that can manage many devices and data sets. Federated learning may also speed up blockchain application development, improve blockchain security and performance, and enable new blockchain-AI fusion applications.

6 Conclusion

This paper comprehensively reviews and summarizes blockchain security threats and collaborative defense. We introduce the classification and threat assessment process of blockchain security threats, investigate the research status of single-node defense technology and multi-node collaborative defense technology, and summarize blockchain security assessment indicators and evaluation methods. First of all, the security defense of the blockchain system is critical, it can protect the integrity, privacy, and trustworthiness of the data. Secondly, single-node defense technology and multi-node collaborative defense technology have their unique advantages and limitations, and it is necessary to choose the appropriate technology to protect the security of the blockchain system according to the actual situation. Third, blockchain security assessment indicators and evaluation methods can help evaluate the security and credibility of blockchain systems and determine corresponding security measures. Finally, future research can focus on improving the efficiency and accuracy of security assessments, while also developing more efficient and reliable defense technologies to address evolving threats and challenges.

Acknowledgement: Not applicable.

Funding Statement: This work was supported by National Natural Science Foundation of China (Grant Nos. 62162022 and 62162024), Young Talents' Science and Technology Innovation Project of Hainan Association for Science and Technology (Grant No. QCXM202007), Hainan Provincial Natural Science Foundation of China (Grant Nos. 2019RC098 and 621RC612).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: X. Li, J. Cheng; data collection: Z. Shi, B. Zhang, B. Xu; analysis and interpretation of results: X. Li, J. Cheng; draft manuscript preparation: X. Tang, V. Sheng. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Chen, H. Chen, Y. Zhang, M. Han, M. Siddula *et al.,* "A survey on blockchain systems: Attacks, defenses, and privacy preservation," *High-Confidence Computing*, vol. 2, no. 2, pp. 100048, 2022.

[2] B. Bhushan, P. Sinha, K. M. Sagayam and J. Andrew, "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions," *Computers & Electrical Engineering*, vol. 90, pp. 106897, 2021.

[3] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan *et al.,* "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[4] M. Touloupou, M. Themistocleous, E. Iosif and K. Christodoulou, "A systematic literature review towards a blockchain benchmarking framework," *IEEE Access*, vol. 10, pp. 70630–70644, 2022.

[5] P. Ekparinya, G. Vincent and J. Guillaume, "Impact of man-in-the-middle attacks on Ethereum," in *2018 IEEE 37th Symp. on Reliable Distributed Systems (SRDS)*, Salvador, Brazil, pp. 11–20, 2018.

[6] J. Cheng, L. Xie, X. Tang, N. Xiong and B. Liu, "A survey of security threats and defense on blockchain," *Multimedia Tools and Applications*, vol. 80, pp. 30623–30652, 2021.

[7] K. Nicolas, Y. Wang, G. C. Giakos, B. Wei and H. Shen, "Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach," *IEEE Access*, vol. 9, pp. 3838–3857, 2020.

[8] C. Killer, B. Rodrigues and B. Stiller, "Security management and visualization in a blockchain-based collaborative defense," in *2019 IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, Seoul, Korea (South), pp. 108–111, 2019.

[9] M. A. Sheikh, G. Z. Khan and F. K. Hussain, "Systematic analysis of DDoS attacks in blockchain," in *2022 24th Int. Conf. Advanced Communication Technology (ICACT)*, Pyeongchang, Korea (South), pp. 132–137, 2022.

[10] Y. Mo and S. Bruno, "Secure control against replay attacks," in *2009 47th Annual Allerton Conf. on Ccommunication, Control, and Computing (Allerton)*, Monticello, IL, USA, pp. 911–918, 2009.

[11] M. Saad, V. Cook, L. Nguyen, M. T. Thai and D. Mohaisen, "Exploring partitioning attacks on the bitcoin network," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 202–214, 2022.

[12] G. Ramezan, C. Leung and Z. J. Wang, "A strong adaptive, strategic double-spending attack on blockchains," in *2018 IEEE Int. Conf. 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)*, Halifax, NS, Canada, pp. 1219–1227, 2018.

[13] F. Farha, H. Ning, S. Yang, J. Xu, W. Zhang *et al.,* "Timestamp scheme to mitigate replay attacks in secure ZigBee networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 1, pp. 342–351, 2022.

[14] Y. Kissoon and G. Bekaroo, "Detecting vulnerabilities in smart contract within blockchain: A review and comparative analysis of key approaches," in *2022 3rd Int. Conf. on Next Generation Computing Applications (NextComp)*, Flic-en-Flac, Mauritius, pp. 1–6, 2022.

[15] R. Henry, A. Herzberg and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 38–45, 2018.

[16] G. Morganti, E. Schiavone and A. Bondavalli, "Risk assessment of blockchain technology," in *2018 Eighth Latin-American Symp. on Dependable Computing (LADC)*, Foz do Iguacu, Brazil, pp. 87–96, 2018.

[17] L. Böck, N. Alexopoulos, E. Saracoglu, M. Mühlhäuser and E. Vasilomanolakis, "Assessing the threat of blockchain-based botnets," in *2019 APWG Symp. on Electronic Crime Research (eCrime)*, Pittsburgh, PA, USA, pp. 1–11, 2019.

[18] M. K. Shrivas, T. Y. Dean and S. S. Brunda, "The disruptive blockchain security threats and threat categorization," in *2020 First Int. Conf. on Power, Control and Computing Technologies (ICPC2T)*, Raipur, India, pp. 327–338, 2020.

[19] S. Zhai, Y. Yang, J. Li, C. Qiu and J. Zhao, "Research on the application of cryptography on the blockchain," *Journal of Physics: Conference Series*, vol. 1168, no. 3, pp. 32077–32085, 2019.

[20] K. Nicolas, Y. Wang, G. C. Giakos, B. Wei and H. Shen, "Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach," *IEEE Access*, vol. 9, pp. 3838–3857, 2021.

[21] S. Ar and B. G. Banik, "A comprehensive study of blockchain services: Future of cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 10, pp. 279–288, 2020.

[22] R. Zhang, R. Xue and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, 2019.

[23] S. Balogh, O. Gallo, R. Ploszek, P. Špaček and P. Zajac, "IoT security challenges: Cloud and blockchain, postquantum cryptography, and evolutionary techniques," *Electronics*, vol. 10, no. 21, pp. 2647–2669, 2021.
[24] S. Kumari, M. Singh, R. Singh and H. Tewari, "Post-quantum cryptography techniques for secure communication in resource-constrained internet of things devices: A comprehensive survey," *Software: Practice and Experience*, vol. 52, no. 3, pp. 2047–2076, 2022.
[25] Z. Yang, H. Zhang, H. Yu, Z. Li, B. Zhu *et al.,* "Attribute-based keyword search over the encrypted blockchain," *Computer Modeling in Engineering & Sciences*, vol. 128, no. 1, pp. 269–282, 2021.
[26] P. S. Chakraborty, M. S. Chandrawanshi, P. Kumar and S. Tripathy, "BSMFS: Blockchain assisted secure multi-keyword fuzzy search over encrypted data," in *2022 IEEE Int. Conf. on Blockchain (Blockchain)*, Espoo, Finland, pp. 216–221, 2022.
[27] R. Bhaskaran1, R. Karuppathal, M. Karthick, J. Vijayalakshmi, S. Kadry *et al.,* "Blockchain enabled optimal lightweight cryptography based image encryption technique for IIoT," *Intelligent Automation & Soft Computing*, vol. 33, no. 3, pp. 1593–1606, 2022.
[28] X. Li, J. Li, F. Yu, X. Fu, J. Yang *et al.,* "BEIR: A blockchain-based encrypted image retrieval scheme," in *2021 IEEE 24th Int. Conf. on Computer Supported Cooperative Work in Design (CSCWD)*, Dalian, China, pp. 452–457, 2021.
[29] B. Zhao and X. Huang, "Encrypted monument: The birth of crypto place on the blockchain," *Geoforum*, vol. 116, pp. 149–152, 2020.
[30] L. Liu, Y. Hu, J. Yu, F. Zhang, G. Huang *et al.,* "Training encrypted models with privacy-preserved data on blockchain," in *Proc. of the 3rd Int. Conf. on Vision, Image and Signal Processing*, Vancouver, BC, Canada, pp. 1–6, 2019.
[31] J. Fu, S. Qiao, Y. Huang, X. Si, B. Li *et al.,* "A study on the optimization of blockchain hashing algorithm based on PRCA," *Security and Communication Networks*, vol. 8, no. 1, pp. 1–12, 2020.
[32] P. Velmurugadass, S. Dhanasekaran, S. S. Anand and V. Vasudevan, "Enhancing blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Materials Today: Proceedings*, vol. 37, pp. 2653–2659, 2021.
[33] X. Xue, C. Wang, W. Liu, H. Lv, M. Wang *et al.,* "A RISC-V processor with area-efficient memristor-based in-memory computing for hash algorithm in blockchain applications," *Micromachines*, vol. 10, no. 8, pp. 541, 2019.
[34] P. Zhang, L. Wang, W. Wang, K. Fu and J. Wang, "A blockchain system based on quantum-resistant digital signature," *Security and Communication Networks*, vol. 1, no. 1, pp. 1–13, 2021.
[35] A. Durand, P. Gremaud and J. Pasquier, "Decentralized LPWAN infrastructure using blockchain and digital signatures, concurrency and computation," *Practice and Experience*, vol. 32, no. 12, pp. 133–139, 2020.
[36] S. Singh, N. K. Rajput, V. K. Rathi, H. M. Pandey, A. K. Jaiswal *et al.,* "Securing blockchain transactions using quantum teleportation and quantum digital signature," *Neural Processing Letters*, vol. 18, pp. 1–16, 2020.
[37] S. G. Liu, W. Q. Chen and J. L. Liu, "An efficient double parameter elliptic curve digital signature algorithm for blockchain," *IEEE Access*, vol. 9, pp. 77058–77066, 2021.
[38] B. Sowmiya, E. Poovammal, K. Ramana, S. Singh and B. Yoon, "Linear elliptical curve digital signature (LECDS) with blockchain approach for enhanced security on cloud server," *IEEE Access*, vol. 9, pp. 138245–138253, 2021.
[39] B. M. Nguyen, T. C. Dao and B. L. Do, "Towards a blockchain-based certificate authentication system in Vietnam," *PeerJ Computer Science*, vol. 6, pp. 367–394, 2020.
[40] Z. Cui, F. Xue, S. Q. Zhang, X. J. Cai, Y. Cao *et al.,* "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.
[41] O. Umoren, R. Singh, S. Awan, Z. Pervez and K. Dahal, "Blockchain-based secure authentication with improved performance for fog computing," *Sensors*, vol. 22, no. 22, pp. 8969–8984, 2022.

[42] S. Liu, Y. Chai, L. Hui and W. Wu, "Blockchain-based anonymous authentication in edge computing environment," *Electronics*, vol. 12, no. 1, pp. 219–236, 2023.
[43] S. Kim, H. J. Mun and S. Hong, "Multi-factor authentication with randomly selected authentication methods with DID on a random terminal," *Applied Sciences*, vol. 12, no. 5, pp. 2301, 2022.
[44] M. Xu, G. Xu, H. Xu, J. Zhou and S. Li, "A decentralized lightweight authentication protocol under blockchain," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 13, pp. 2067–2087, 2022.
[45] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.
[46] J. Li, J. Wu, L. Chen, J. Li and S. K. Lam, "Blockchain-based secure key management for mobile edge computing," *IEEE Transactions on Mobile Computing*, vol. 22, no. 1, pp. 100–114, 2023.
[47] V. Ribeiro, R. Holanda, A. Ramos and J. J. Rodrigues, "Enhancing key management in LoRaWAN with permissioned blockchain," *Sensors*, vol. 20, no. 11, pp. 3068–3084, 2020.
[48] T. Zhou, J. Shen, Y. Ren and S. Ji, "Threshold key management scheme for blockchain-based intelligent transportation systems," *Security and Communication Networks*, vol. 2021, pp. 1–8, 2021.
[49] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah *et al.,* "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.
[50] A. Singh and B. B. Gupta, "Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, no. 1, pp. 1–43, 2022.
[51] C. Killer, B. Rodrigues and B. Stiller, "Threat management dashboard for a blockchain collaborative defense," in *2019 IEEE Globecom Workshops (GC Wkshps)*, Waikoloa, HI, USA, pp. 1–6, 2019.
[52] A. Gruhler, B. Rodrigues and B. Stiller, "A reputation scheme for a blockchain-based network cooperative defense," in *2019 IFIP/IEEE Symp. on Integrated Network and Service Management (IM)*, Arlington, VA, USA, pp. 71–79, 2019.
[53] M. Hajizadeh, N. Afraz, M. Ruffini and T. Bauschert, "Collaborative cyber attack defense in SDN networks using blockchain technology," in *2020 6th IEEE Conf. on Network Softwarization (NetSoft)*, Ghent, Belgium, pp. 487–492, 2020.
[54] G. Ahmadi-Assalemi, H. M. al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani *et al.,* "Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace," in *2019 IEEE 12th Int. Conf. on Global Security, Safety and Sustainability (ICGS3)*, London, UK, pp. 1–9, 2019.
[55] G. Sagirlar, B. Carminati and E. Ferrari, "AutoBotCatcher: Blockchain-based P2P botnet detection for the internet of things," in *2018 IEEE 4th Int. Conf. on Collaboration and Internet Computing (CIC)*, Philadelphia, PA, USA, pp. 1–8, 2018.
[56] Z. A. El Houda, A. Hafid and L. Khoukhi, "Co-IoT: A collaborative DDoS, itigation scheme in IoT environment based on blockchain using SDN," in *2019 IEEE Global Communications Conf. (GLOBECOM)*, Waikoloa, HI, USA, pp. 1–6, 2019.
[57] A. Febro, H. Xiao, J. Spring and B. Christianson, "Synchronizing DDoS defense at network edge with P4, SDN, and Blockchain," *Computer Networks*, vol. 216, pp. 109267, 2022.
[58] B. Rodrigues, S. Trendafilov, E. Scheid and B. Stiller, "SC-FLARE: Cooperative DDoS signaling based on smart contracts," in *2020 IEEE Int. Conf. on Blockchain and Cryptocurrency (ICBC)*, Toronto, ON, Canada, pp. 1–3, 2020.
[59] F. Zhang and Y. Huang, "Trusted computing in power distribution IoT: A fuzzy set theory based analysis," *Journal of Intelligent & Fuzzy Systems*, vol. 41, no. 4, pp. 4883–4889, 2021.
[60] D. Kim, C. Oh and Y. Zhu, "Analyzing research trends in blockchain studies in South Korea using dynamic topic modeling and network analysis," *Journal of the Korean Society for Information Management*, vol. 38, no. 3, pp. 23–39, 2021.

[61] W. Guo, J. Xu, Y. Pei, L. Yin, C. Jiang *et al.,* "A distributed collaborative entrance defense framework against DDoS attacks on satellite internet," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 15497–15510, 2022.
[62] S. Rahmadika and K. H. Rhee, "Enhancing data privacy through a decentralized predictive model with blockchain-based revenue," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 37, no. 1, pp. 1–15, 2021.
[63] L. Shi, X. Li, Z. Gao, P. Duan, N. Liu *et al.,* "Worm computing: A blockchain-based resource sharing and cybersecurity framework," *Journal of Network and Computer Applications*, vol. 185, no. 1, pp. 103081, 2021.
[64] S. Jiang, L. Yang, X. Gao, Y. Zhou, T. Feng *et al.,* "BSD-guard: A collaborative blockchain-based approach for detection and mitigation of sdn-targeted ddos attacks," *Security and Communication Networks*, vol. 2022, pp. 1–16, 2022.
[65] R. Saxena and E. Gayathri, "Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution," *Materials Today: Proceedings*, vol. 51, pp. 682–689, 2022.
[66] M. Essaid, D. Kim, S. H. Maeng, S. Park and H. T. Ju, "A collaborative DDoS mitigation solution based on Ethereum smart contract and RNN-LSTM," in *2019 20th Asia-Pacific Network Operations and Management Symp. (APNOMS)*, Matsue, Japan, pp. 1–6, 2019.
[67] A. Pavlidis, M. Dimolianis, K. Giotis, L. Anagnostou, N. Kostopoulos *et al.,* "Orchestrating DDoS mitigation via blockchain-based network provider collaborations," *The Knowledge Engineering Review*, vol. 35, pp. e16, 2020.
[68] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng *et al.,* "A blockchain-based decentralized federated learning framework with committee consensus," *IEEE Network*, vol. 35, no. 1, pp. 234–241, 2021.
[69] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato *et al.,* "A secure federated learning framework for 5G networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 24–31, 2020.
[70] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato *et al.,* "Privacy-preserving blockchain-based federated learning for IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1817–1829, 2020.
[71] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu *et al.,* "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5171–5183, 2020.
[72] H. Kim, J. Park, M. Bennis and S. L. Kim, "Blockchained on-device federated learning," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, 2020.
[73] Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020.
[74] U. Majeed and C. S. Hong, "FLchain: Federated learning via MEC-enabled blockchain network," in *2019 20th Asia-Pacific Network Operations and Management Symp. (APNOMS)*, Matsue, Japan, pp. 1–4, 2019.
[75] X. Cheng, W. Tian, F. Shi, M. Zhao, S. Chen *et al.,* "A blockchain-empowered cluster-based federated learning model for blade icing estimation on IoT-enabled wind turbine," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9184–9195, 2022.
[76] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao *et al.,* "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, 2021.
[77] I. Makhdoom, K. Hayawi, M. Kaosar, S. S. Mathew and P. H. Ho, "D2Gen: A decentralized device genome based integrity verification mechanism for collaborative intrusion detection systems," *IEEE Access*, vol. 9, pp. 137260–137280, 2021.
[78] M. Tayyab, B. Belaton and M. Anbar, "ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review," *IEEE Access*, vol. 8, pp. 170529–170547, 2020.
[79] P. Banerjee, B. Kumar, A. Singh, H. Prasad and B. Raj, "A review of usability and security evaluation model of blockchain technologies," *International Journal of Computer Techniques*, vol. 7, no. 2, pp. 235–246, 2020.

[80] R. Kalis and A. Belloum, "Validating data integrity with blockchain," in *2018 IEEE Int. Conf. on Cloud Computing Technology and Science (CloudCom)*, Nicosia, Cyprus, pp. 272–277, 2018.
[81] Z. Cui, X. U. E. Fei, S. Zhang, X. Cai, Y. Cao *et al.,* "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.
[82] C. Stach, C. Gritti, D. Przytarski and B. Mitschang, "Assessment and treatment of privacy issues in blockchain systems," *ACM SIGAPP Applied Computing Review*, vol. 22, no. 3, pp. 5–24, 2022.
[83] X. Han and Y. Liu, "Research on the consensus mechanisms of blockchain technology," *Netinfo Security*, vol. 5, no. 9, pp. 147–152, 2017.
[84] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur and H. N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605–6621, 2022.
[85] M. Panda, "Performance analysis of encryption algorithms for security," in *2016 Int. Conf. on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, India, pp. 278–284, 2016.
[86] M. Abbas, M. Rashid, F. Azam, Y. Rasheed, M. W. Anwar *et al.,* "A model-driven framework for security labs using blockchain methodology," in *2021 IEEE Int. Systems Conf. (SysCon)*, Melbourne, Australia, pp. 1–7, 2021.
[87] A. van Moorsel, "Benchmarks and models for blockchain," in *Proc. of the 2018 ACM/SPEC Int. Conf. on Performance Engineering*, New York, NY, USA, pp. 3, 2018.
[88] N. Papadis, S. Borst, A. Walid, M. Grissa and L. Tassiulas, "Stochastic models and wide-area network measurements for blockchain design and analysis," in *IEEE INFOCOM 2018-IEEE Conf. on Computer Communications*, London, UK, pp. 2546–2554, 2018.
[89] S. Zafar, Z. Alamgir and M. H. Rehman, "An effective blockchain evaluation system based on entropy-CRITIC weight method and MCDM techniques," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 3110–3123, 2021.
[90] K. Tsoulias, G. Palaiokrassas, G. Fragkos, A. Litke and T. A. Varvarigou, "A graph model based blockchain implementation for increasing performance and security in decentralized ledger systems," *IEEE Access*, vol. 8, pp. 130952–130965, 2020.
[91] S. M. H. Bamakan, A. Motavali and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154, pp. 113385, 2020.
[92] S. Smetanin, A. Ometov, M. Komarov, P. Masek and Y. Koucheryavy, "Blockchain evaluation approaches: State-of-the-art and future perspective," *Sensors*, vol. 20, no. 12, pp. 3358, 2020.
[93] S. Gaur and N. Rahman, "A secured log mining approach to collection, monitoring, rotation, and analysis of frequent and heterogeneous logs," in *Proc. of the 2nd Int. Conf. ICT for Digital, Smart, and Sustainable Development (ICIDSSD)*, New Delhi, India, vol. 285, 2020.
[94] Z. Yan, "Network data collection, fusion, mining and analytics for cyber security," in *Machine Learning for Cyber Security: Second Int. Conf.*, Guangzhou, China, pp. 1–5, 2019.
[95] W. T. Tsai, R. Wang, S. Liu, E. Deng and D. Yang, "COMPASS: A data-driven blockchain evaluation framwework," in *2020 IEEE Int. Conf. on Service Oriented Systems Engineering (SOSE)*, Oxford, UK, pp. 17–30, 2020.
[96] B. Su, C. Liu, Y. Li, Q. Zhang and H. Zhang, "Safety exploration and analysis of the computer data based on the block chain technology," in *2022 2nd Asia-Pacific Conf. on Communications Technology and Computer Science (ACCTCS)*, Shenyang, China, pp. 148–151, 2022.
[97] B. Putz and G. Pernul, "Detecting blockchain security threats," in *2020 IEEE Int. Conf. on Blockchain (Blockchain)*, Rhodes, Greece, pp. 313–320, 2020.
[98] P. K. Bharimalla, S. Praharaj and S. R. Dash, "ANN based block chain security threat mechanism," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 10, pp. 2672–2679, 2019.
[99] S. T. Abdulrazzaq, F. S. Omar and M. A. Mustafa, "Decentralized security and data integrity of blockchain using deep learning techniques," *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 3, pp. 1911–1923, 2020.

[100] S. Gaba, I. Budhiraja, A. Makkar and D. Garg, "Machine learning for detecting security attacks on blockchain using software defined networking," in *2022 IEEE Int. Conf. on Communications Workshops (ICC Workshops)*, Seoul, Korea, pp. 260–264, 2022.
[101] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat *et al.,* "Security implications of blockchain cloud with analysis of block withholding attack," in *17th IEEE/ACM Int. Symp. on Cluster, Cloud and Grid Computing (CCGRID)*, Madrid, Spain, pp. 458–467, 2017.
[102] D. Marmsoler and L. Eichhorn, "Simulation-based analysis of blockchain architectures," in *The 3rd Symp. on Distributed Ledger Technology (SDLT 3)*, Gold Coast, Australia, 2018.
[103] M. Alharby and A. Van Moorsel, "Blocksim: A simulation framework for blockchain systems," *ACM Sigmetrics Performance Evaluation Review*, vol. 46, no. 3, pp. 135–138, 2019.
[104] J. Kreku, V. A. Vallivaara, K. Halunen, J. Suomalainen, M. Ramachandran *et al.,* "Evaluating the efficiency of blockchains in IoT with simulations," in *IoTBDS*, vol. 820, pp. 216–223, 2017.
[105] B. Wang, S. Chen, L. Yao, B. Liu, X. Xu *et al.,* "A simulation approach for studying behavior and quality of blockchain networks," in *Blockchain–ICBC 2018*, Seattle, WA, USA, pp. 18–31, 2018.
[106] R. A. Memon, J. P. Li and J. Ahmed, "Simulation model for blockchain systems using queuing theory," *Electronics*, vol. 30, no. 2, pp. 234, 2019.
[107] D. K. Gouda, S. Jolly and K. Kapoor, "Design and validation of blockeval, a blockchain simulator," in *2021 Int. Conf. on COMmunication Systems & NETworkS (COMSNETS)*, Bengaluru, India, pp. 281–289, 2021.
[108] A. Maheshwari, B. Mehraj, M. S. Khan and M. S. Idrisi, "An optimized weighted voting based ensemble model for DDoS attack detection and mitigation in SDN environment," *Microprocessors and Microsystems*, vol. 89, pp. 104412, 2022.