Journal of Intelligent System and Applied Data Science (JISADS)

Journal homepage : https://www.jisads.com

ISSN (2974-9840) Online

BLOCKCHAIN BEYOND TECHNOLOGY: EXPLORING APPLICATIONS, COLLABORATIVE INNOVATIONS, AND GOVERNANCE STRATEGIES

Ihab Adib[1] *and Youjun Liu*[1*]

College of Life Science and Bio-Engineering, Beijing University of Technology, No. 100 Pingleyuan, Chaoyang District, Beijing 100124, China.

Ihab.s.adib@gmail.com, lyjlma@bjut.edu.cn

ABSTRACT

Blockchain is a new distributed computing paradigm characterized by security and trust, widely applied in various fields. However, security issues have become increasingly prominent, and the need for regulation is more urgent. The current state of the blockchain ecosystem and the regulatory policy backgrounds of major countries were briefly introduced. The relevant literature based on blockchain technology and application architecture were categorized and the characteristics of existing regulatory technologies and solutions were analyzed from three aspects: intra-chain regulation, inter-chain regulation, and off-chain regulation. Intra-chain regulation was further divided into three levels: infrastructure layer regulation, core function layer regulation, and user layer regulation. The advantages and disadvantages of different regulatory technologies at each level were discussed in detail. Inter-chain regulation was divided into two categories: regulation based on the "governance by chain" concept and cross-chain security regulation, with a brief discussion of the characteristics of related studies. Then some representative cases of off-chain regulation were introduced. Finally, the common issues in current blockchain security regulation were analyzed with possible improvement directions and new areas in need of regulation. The gap was filled in reviews on blockchain regulation and a reference for the design of blockchain regulatory solutions was provided.

Keywords: blockchain; blockchain security; blockchain regulation, Classification

1. INTRODUCTION

Since its inception, blockchain has evolved from Blockchain 1.0 to Blockchain 3.0, and its application scope has expanded from single payment scenarios to multiple industries, such as financial services, government and legal affairs, supply chain management, and identity verification [1]. Blockchain 1.0 focused on digital currencies, achieving decentralized value transfer. Blockchain 2.0 introduced smart contracts, marking the realization of complex business logic execution on-chain. Blockchain 3.0 emphasizes applying blockchain to real-world scenarios, realizing decentralized commercial networks [2].

In recent years, the rapid development of blockchain has led to increasingly rich blockchain applications. A batch of emerging blockchain projects represented by high-performance public chains has emerged, such as Solana [3], Avax [4], Near, Hedera [5], Sui [6], etc. Traditional public chains (such as Bitcoin, Ethereum, Binance Chain, etc.) have also attracted a large influx of funds, incubating various Web3 projects, such as decentralized exchanges (DEX) [7], decentralized social and chat software [8], inscription and rune protocols, blockchain games [9], Web3 cloud services [10], etc. [11-16].

With the explosive growth of blockchain technology applications, its security issues have also become prominent. The risks caused by vulnerabilities in underlying blockchain platforms and blockchain applications, as well as various virtual asset crimes, pose

great challenges to blockchain security. According to SlowMist Hacked Statistical database, the number of major public security incidents in global blockchain has shown an increasing trend year by year since 2012, as shown in Figure 1. Blockchain-related security incidents mainly include 9 categories: wallet security incidents, malicious mining, distributed denial-of-service (DDoS) attacks, ransomware, digital currency fraud, digital currency money laundering, smart contract security, exchange security, and other attack incidents [17-18].

With frequent blockchain security incidents, the demand for strengthening blockchain regulation is becoming increasingly urgent. Since 2019, although the number of blockchain-related literature included in databases such as IEEE, ACM, and Springer has reached more than 74,000, there are very few reviews directly studying blockchain regulation. Currently, domestic and foreign reviews related to blockchain regulation [19-22] tend to focus on the analysis of blockchain security or vulnerability detection and defense, or some related literature analyzes blockchain security in certain specific application scenarios [23-29], but does not involve blockchain regulation.

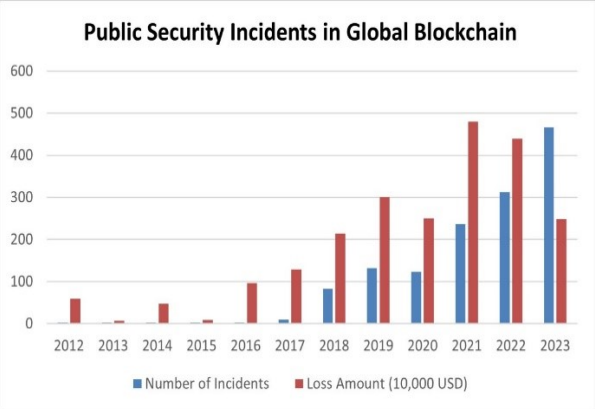

Figure1. Puplic security incedents in Global Blockchain

Based on the current development status of blockchain technology architecture, this paper divides it and the applications running on it into three layers: intra-chain infrastructure, cross-chain expansion, and decentralized autonomous communities and applications. The main contributions of this paper are as follows:

1) The existing regulatory schemes are summarized into intra-chain regulation, inter-chain regulation, and off-chain regulation. Intra-chain regulation is further divided into three levels: infrastructure layer regulation, core function layer regulation, and user layer regulation, and the advantages and disadvantages of regulatory technologies at each level are meticulously classified according to the focus of relevant literature.

2) Inter-chain regulation is further divided into regulation based on the "governance by chain" concept and cross-chain security regulation, analyzing and comparing the characteristics of related literature, and briefly discussing representative cases of off-chain regulation.

3) Common issues in existing regulation are analyzed, and possible improvement directions are provided, pointing out that regulation should focus on emerging blockchain projects represented by Rollup and decentralized finance (DeFi) projects.

1. Blockchain Regulation Background

With the in-depth development of blockchain technology, its application scenarios have gradually enriched, and various complex applications have gradually formed the embryonic form of the blockchain ecosystem. These ecological projects have attracted a continuous influx of massive funds, and at the same time, they have also attracted the attention of governments and organizations around the world. This section briefly introduces the current state of the blockchain ecosystem and the representative blockchain regulatory policies of major countries.

1.1 Current State of the Blockchain Ecosystem

In academia, some literature has proposed the concept of blockchain ecosystem [24-30,145]. After summarizing relevant literature [31-33], the composition of the blockchain ecosystem is shown in Figure 2. The bottom layer of Figure 3 is the supporting development technology, and breakthroughs often promote the innovation of blockchain technology, usually computer basic disciplines or technologies such as cryptography, big data, distributed systems, cloud and fog computing, and decentralized learning. The top-level application areas include real-world assets (RWA), electronic auctions, lending, decentralized finance, and many other scenarios. The blockchain ecosystem entities consist of eight parts: blockchain users, blockchain application providers, blockchain platform service providers, blockchain infrastructure, blockchain communities, blockchain equipment providers, blockchain regulatory agencies, and blockchain technology consulting providers [34-35]. These components are interconnected and interact through data and funds, forming an interdependent and mutually influential whole.

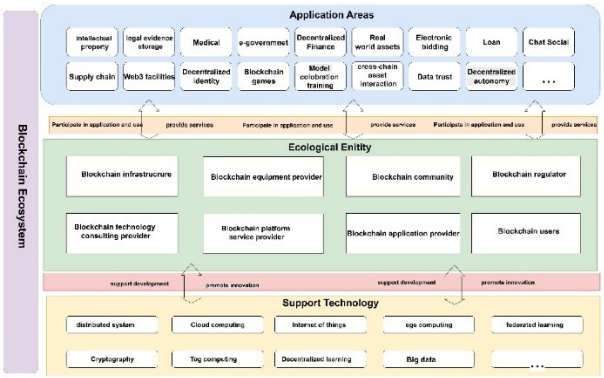

Figure 2. Blockchain ecosystem composition

1.2 Blockchain Regulatory Policies Beyond academic research, blockchain has received varying degrees of attention from governments and organizations worldwide during its development. Some countries and organizations have already carried out systematic and standardized blockchain security regulation work [36-37], and relevant regulatory policies and regulatory agencies are shown in Table 1.

Table 1: Blockchain-related regulatory policies and regulatory agencies of some countries and organizations

Canada	Canadian Cryptocurrency Tax Guide	Canada Revenue Agency (CRA)
France	Regulatory framework related to crypto assets and licensing requirements and regulations for digital asset service providers	French Financial Supervisory Authority (AMF); Association for the Development of Digital Assets (ADAN)
Singapore	Fiatech Regulatory Standard Guidelines, Digital Asset Taxation Act and Financial Institutions Code of Conduct	Monetary Authority of Singapore (MAS); Personal Data Protection Commission (PPDC); Intellectual Property Office of Singapore (IPOS)
China	Notice on Preventing Bitcoin Risks, Announcement on Preventing Token Issuance and Financing Risks, Blockchain Security White Paper, Blockchain Information Service Management Regulations and Financial Information Service Management Regulations	Cyberspace Administration of China; Digital Currency Research Institute of the People's Bank of China; Blockchain Committee of Internet Society of China (SEC)
Japan	Digital Finance Strategy, Blockchain Strategy, General Data Protection Regulation and EU Fintech Action Plan	European Securities and Markets Authority (ESMA); European Banking Authority (EBA); European Data Protection Supervisor (EDPS)
Germany	Digital Currency Exchange Act, Payment Services Act, Proposal on New ECO Regulation and Asset Settlement Act Enforcement Decree	Financial Services Agency of Japan (FAS), Japan Blockchain Association (LIRA), Japan Virtual Currency Exchange Association (JVCEA)
IMF	Crypto-assets, regulatory challenges in the global economy and regulatory frameworks for digital financial services. International Monetary Fund (IMF)	Federal Financial Supervisory Authority (BaFin); Federal Commissioner for Data Protection and Freedom of Information (BFDI); Financial Market Stability Fund (SoFFin)

The UK government first proposed the concept of a "regulatory sandbox" [38]. The United States has formulated intellectual property and tax regulations for blockchain technology and digital assets and established a blockchain industry alliance to promote the development and regulation of the blockchain industry [39]. The European Commission has formulated the "Digital Finance Strategy 2020" and "Blockchain Strategy" to strengthen regulation and cooperation in the digital finance field. The Singapore government has issued a digital asset tax law, stipulating that digital asset transactions should be taxed [40]. Switzerland has formulated a series of blockchain laws and policies [41] to provide legal protection, guidance, and regulation for blockchain enterprises. At the same time, it has also strengthened support and regulation of the blockchain industry, encouraging enterprises to develop more secure blockchain technology. In 2019, the Ministry of Industry and Information Technology established the National Blockchain and Distributed Ledger Technology Standardization Committee to systematically promote standardization work and accelerate the establishment of a blockchain regulatory system.

2. BLOCKCHAIN REGULATION AND CLASSIFICATION

Research progress on blockchain security and regulation at home and abroad is shown in Table 2. Literature [20-22, 45-49] focuses on the research of blockchain data security and network security issues, and does not discuss the overall regulation of blockchain. Literature [23-25, 50-56] focuses on discussing blockchain-specific security issues such as smart contract vulnerabilities and consensus algorithm vulnerabilities. In addition to the reviews listed in Table 2, there is also literature discussing the development of the blockchain ecosystem [26-30, 57], but it does not discuss blockchain security regulation.

This paper divides existing blockchain regulatory schemes and literature into intra-chain regulation, inter-chain regulation, and off-chain regulation. Intra-chain regulation consists of blockchain infrastructure layer regulation, core function layer regulation, and user layer regulation. It involves a large number of literatures [58-118] and is a key level of regulation. Inter-chain regulation consists of two types: regulation based on the "governance by chain" concept and cross-chain security regulation [119-131]. Off-chain regulation mainly involves decentralized autonomous organizations (DAO) and communities. Due to the short development history of cross-chain technology and off-chain decentralized governance mechanisms, there are fewer related literatures and regulatory schemes [132-137].

Table 2: Research progress on blockchain security and regulation

Literature	**Focus**	**Does it involve supervision?**
References[20-22,45]	Blockchain security, uncertainty, status of additional safeguards analyzed	Not involved
References[46-48]	Blockchain data security, network security, etc.	Not comprehensive
Literature[49]	Blockchain application research	Not involved
References[50-53]	Smart contract vulnerability detection and repair	Not involved
References[23-25,55-56]	Constraints mechanism security improvements	Not involved

2.1 Intra-chain Regulation

This section divides intra-chain regulation into three layers: infrastructure layer regulation, core function layer regulation, and user layer regulation. The regulatory technologies at the infrastructure layer are further divided into node association tracking, node abnormal behavior detection, and node attack traffic detection. The regulatory technologies at the core function layer are divided into abnormal transaction analysis and detection, smart contract security detection, consensus mechanism attack detection, and consortium chain penetration regulation. User layer regulation mainly targets users, including user business regulation and user account regulation.

2.1.1 Infrastructure Layer Regulation The infrastructure layer provides the necessary hardware components and operating environment to support the normal operation of the entire blockchain system, mainly including computing resources for storing blockchain data and executing blockchain computing tasks, backup and recovery mechanisms, and other security and protection measures to ensure the connectivity and data transmission stability of the network infrastructure between nodes.

2.1.1.1 Node Association Tracking Technology Blockchain node tracking technology refers to collecting and analyzing information such as network addresses, account addresses, and transactions of nodes in the blockchain network to construct the association relationship and topological structure between nodes, thereby understanding the connection methods, interaction situations, and transaction behavior characteristics between nodes, and achieving security regulation of the blockchain. Node association tracking technology does not affect the final state of transactions and blockchain, and belongs to ex-post regulation.

Related research [58-60] mainly uses graph analysis and log analysis, machine learning, and cluster analysis to track blockchain transactions, ultimately clarifying the relationship between blockchain nodes. The current difficulty is tracking highly private cryptocurrency transactions.

Graph analysis and log analysis audit. In response to the limitations of tracking analysis technology based on pollution/dyeing mentioned in literature [58-60] in terms of effectiveness, universality, and efficiency, Li Zhiyuan et al. [61] proposed a blockchain transaction tracking method based on node influence account balance model, which uses network analysis and graph data mining technology to track the flow of funds of specific target accounts through the account balance model, compensating for the shortcomings and deficiencies of existing blockchain transaction tracking research in terms of universality and efficiency. Focusing on the process tracking of consensus transactions, Li Shanshan et al. [62] proposed a Fabric consensus transaction trajectory tracking method based on custom logs, which uses the ELK (Elasticsearch Logstash Kibana) tool chain to collect and parse Fabric's custom consensus transaction logs, and processes custom log business logic through a Spring Boot backend application, which can effectively track the call trajectory of Fabric's consensus transactions at each node, realizing the visualization of consensus transaction trajectories. Focusing on node automatic discovery, literature [63] proposed a node automatic discovery mechanism based on the Kademlia protocol. The constructed routing table allows nodes in the network to gradually join their routing tables when discovered by other nodes, thereby realizing dynamic perception of the entire network by nodes.

Machine learning and cluster analysis. Using machine learning methods for blockchain node tracking can improve the efficiency and accuracy of tracking. Machine learning models can learn patterns and rules from a large amount of data, helping to identify and analyze complex node behaviors and relationships. Michalski et al. [64] used supervised learning methods to analyze the characteristics of nodes in the blockchain. By analyzing the behavioral characteristics of nodes in the blockchain network, they inferred the roles played by nodes in the blockchain, such as miners or exchanges. Although the goal of this paper is more focused on locating the roles and behaviors of nodes, its results can provide some help and clues for node tracking. Forward transaction tracking is a common technology used to analyze Bitcoin abuse and track fund flows, that is, starting from a given set of seed addresses known to belong to cybercrime activities, tracking the movement of Bitcoin, but it only considers forward transaction flows, and does not consider backward transaction flows, which means that in some cases, some important relationships and transaction information may be missed. In order to focus on both output transactions and input transactions when analyzing transactions, Gomez et al. [65] proposed a bidirectional exploration automated Bitcoin transaction tracking technology, which outputs a transaction graph from a given seed address belonging to cybercrime activities, and identifies the relationship paths between node activities and external services and other cybercrime activities. In order to prevent the transaction graph from expanding, this technology combines a labeled database with a machine learning classifier to quickly identify and filter out addresses belonging to exchanges. From the perspective of link prediction between nodes, Du et al. [66] proposed a graph neural network framework MixBroker, which uses original Ethereum mixed transaction data to construct a mixed currency interaction graph, and extracts account node features from the graph from multiple perspectives to better represent the attributes of mixed currency account nodes. The graph neural network is used to calculate the correlation probability between nodes, thereby determining the association relationship between mixed currency account nodes, which to a certain extent breaks the anonymity of Ethereum mixed currency services.

In addition, in order to provide a higher level of privacy and anonymity protection, some cryptocurrencies use ring signatures, zero-knowledge proofs, coin mixing, and other technical means to hide the addresses of both parties to the transaction and the transaction amount, such as Monero [67], Zcash [68], and Dash. Although these anonymous coins can provide a certain degree of anonymity and privacy protection, they are not untraceable. There are currently 6 types of Zcash [68] tracking technologies: Danan gift attack, dust attack, remote side-channel attack, round-trip transaction attack, user behavior analysis attack, and covert channel attack, which can be used to infer and track the transaction information of Zcash nodes. In the field of Monero [67] technology tracking, there are currently four main types of tracking methods: tracking based on input-output relationships [69] (such as 0-mixin attack, output merging attack, closed set attack, etc.), tracking based on statistical laws (such as latest guess attack, etc.), tracking with partially known public keys (such as flooding attack, wallet ring attack, etc.), and tracking using Monero's security mechanism vulnerabilities (such as malicious remote node attack, etc.).

2.1.1.2 Node Abnormal Behavior Detection Technology Blockchain nodes may attempt to perform malicious operations, attack networks, phish, tamper with data, or engage in fraudulent activities. Node detection refers to analyzing and monitoring node behavior in the blockchain network to identify possible malicious nodes or abnormal behaviors, and belongs to ex-ante regulation. Node detection methods are diverse, and currently mainly focus on traffic analysis and phishing node detection.

In terms of traffic analysis, Liu Guozhi [70] proposed an abnormal traffic detection algorithm based on federated learning and representation learning, and implemented a distributed abnormal traffic detection system for detecting abnormal nodes in the blockchain network. This system can automatically learn traffic data features, allow participants to dynamically enter and exit, and control the entire process through smart contracts. Unlike literature [70], which focuses on abnormal detection through specific algorithms and systems, Sanda et al. [71] used deep learning convolutional neural networks (CNN), K-nearest neighbors (KNN), decision trees, and multi-layer perceptrons (MLP) algorithms to determine classifiers and predict malicious nodes, which can be further extended to analyze abnormal behavior of verification nodes in proof of stake (PoS) consensus.

In terms of phishing node detection, current methods for detecting Ethereum network phishing mainly focus on transaction features and local network structure, but have limitations in handling complex interactions between edges and large graphs. In response to this problem, Zhang et al. [72] proposed an Ethereum phishing node detection method based on graph convolutional networks (GCN), which converts complex transaction networks into three simple inter-node graphs, and uses GCN to generate node embeddings and global structural information to identify phishing nodes. Similarly, Yu et al. [73] used a message-passing based GCN to first construct a transaction network, and then extract and classify node information to detect phishing nodes. Both of these works use GCN to detect Ethereum phishing nodes, and both involve the processing of transaction networks and the use of node information, which solves the limitations of current detection methods in handling complex interactions and large graphs, and improves the effectiveness and accuracy of detection. However, the former mainly focuses on using GCN to generate node embeddings and global structural information to identify

phishing nodes, while the latter focuses on first constructing a transaction network, and then extracting and classifying node information.

By timely identifying and responding to malicious nodes, abnormal behaviors, and potential risks, the anti-attack capability of blockchain systems can be enhanced, and a more reliable infrastructure can be provided for various application scenarios. However, node detection technology still faces some challenges, such as insufficient privacy protection during detection, low detection efficiency, and low accuracy.

2.1.1.3 Node Attack Traffic Detection Technology At the infrastructure layer, attacks that significantly harm the normal operation of blockchain nodes include Eclipse attacks [74] and DDoS attacks [76], whose purpose is to destroy the availability and functionality of the underlying network infrastructure. Researchers have proposed various detection methods based on deep learning to extract attack features from traffic data, focusing on how to identify and defend against attacks on blockchain infrastructure to ensure its stable and secure operation.

Eclipse Attack Detection Eclipse attacks rely on the cooperation of multiple nodes. By controlling the network connections of target nodes, the target nodes are isolated from other honest nodes. The client cannot distinguish between the canonical view of the blockchain and the view provided by the attacker. This attack has the characteristics of concealment and concurrency. Currently, most existing methods use custom behavior features and deep learning [74], immunity-based abnormal detection methods [77], suspicious timestamp-based detection methods, and communication using blockchain clients [78] to detect Eclipse attacks. In order to more accurately describe the behavioral characteristics of attack traffic, Dai et al. [74] enhanced the detection capability for Eclipse attack traffic by defining multi-level traffic features, improving the upsampling algorithm, and combining deep learning models, using CNN and bidirectional long short-term memory (Bi-LSTM) networks to extract deep features from Eclipse attack traffic, and integrating the feature extraction results into hybrid features through a multi-head attention mechanism. Detection based on suspicious block timestamps refers to determining whether the network is segmented by detecting the time interval between newly created blocks, but this method requires about 2-3 hours to relatively confirm whether the client is under attack. In order to reduce the average attack detection time, Alangot et al. [78] proposed that Bitcoin clients pass messages by establishing connections with servers on the Internet to exchange their blockchain views, and this method does not require introducing any dedicated infrastructure or changing the Bitcoin protocol and network.

Erebus Attack Detection Erebus attacks mainly target blockchain systems that use proof of work (PoW) consensus. Attackers interfere with the normal operation of target nodes by controlling a large number of IP addresses to form a fake network. In response to the problems of single detection objects, weak dynamic attack target perception, and high node resource requirements in existing methods, Dai et al. [75] designed a two-stage feature selection algorithm based on ReliefF_WMRmR and a multi-modal classification detection model based on deep learning by combining traffic behavior features with routing states based on multi-modal deep feature learning, and constructed a multi-modal neural network based on MLP, which can effectively detect Erebus attacks with high accuracy.

DDoS Attack Detection In terms of DDoS attack detection, Dai et al. [76] combined statistical and machine learning methods. By capturing traffic data at the node end of the blockchain network, cross-layer convolution operations are performed on the pre-processed traffic to extract abstract features of highly robust attack traffic, and an improved stochastic gradient descent algorithm is used to globally optimize the model parameters to prevent training parameter oscillation. Link flooding attack (LFA) is a new type of DDoS attack that uses low-rate traffic to flood a part of target links in the blockchain network to block normal traffic passing through these links and cut off the connection between the server and the network. In response to LFA, literature [79] used the time series prediction capability of long short-term memory networks to detect LFA, but whether it can accurately identify suspicious attack sources by calculating the similarity of different traffic sources remains to be further verified.

In addition, the visualization services and tools inherent in blockchain can be used as auxiliary tools for node association tracking and attack traffic detection. For example, blockchain browsers and data analysis tools such as Gephi, Cytoscape, Tokenview, and BlockAPI clearly present the transaction relationships or data interaction relationships between nodes or accounts.

In summary, for infrastructure layer regulation, blockchain node association tracking and detection technologies are mainly divided into two categories: one is to track their activities by monitoring message passing and transaction broadcasting between nodes in the blockchain network. Regulators can collect and analyze these data to understand node behavior patterns, network topology, and transaction flow; the other is to use data visualization technology to dynamically perceive the entire blockchain network through the routing table in blockchain nodes. Regulators can intuitively observe the connection relationships between nodes, transaction flows, and data changes. For the former, abnormal behaviors with defined detection rules can achieve relatively ideal results through data analysis. However, once new abnormal behaviors occur, new transaction datasets need to be organized and detection algorithms need to be redesigned for calculation, which has poor adaptability. The latter relies on data synchronization,

and it must be ensured that each node can achieve data consistency at a certain time. By dynamically visualizing operations to construct knowledge graphs, abnormal address clusters or nodes can be clearly discovered, making it easier to regulate these address clusters or nodes.

Overall, researchers tend to combine multiple technical means, especially graph analysis and machine learning, to achieve more intelligent node tracking and visualization at the infrastructure layer to improve the efficiency of blockchain regulation and the clarity of node relationships. Existing research explores how to improve the efficiency and accuracy of blockchain node tracking and detection. Some research focuses on specific tracking technologies and visualization methods, such as improving the efficiency of node tracking based on graph data mining, machine learning, and other technologies. Other research explores technical means to detect and defend against malicious nodes in different types of attacks (such as Eclipse attacks, DDoS attacks). The common goal of these studies is to enhance the security and regulability of blockchain networks, forming a multi-level, comprehensive node tracking and visualization framework. Future research directions may focus on improving the universality and efficiency of tracking technologies, exploring more secure and private tracking technologies, and further enhancing the security and robustness of blockchain networks.

2.1.2 Core Function Layer Regulation

The core function layer usually consists of core components such as transaction storage, transaction processing, and smart contracts, which are used to implement the basic functions and characteristics of the blockchain and provide reliable basic support for the user layer. The main regulatory methods are abnormal transaction analysis and detection, smart contract security detection, and consensus mechanism attack detection. In addition, consortium chains can achieve penetration regulation at the core function layer.

2.1.2.1 Abnormal Transaction Analysis and Detection Core function layer regulation mainly focuses on transaction data on the blockchain and the execution of smart contracts. Researchers have proposed various data analysis methods to analyze and detect on-chain data. A common method is to identify abnormal transactions and potential fraudulent behaviors based on data mining and machine learning technologies. Regulators can build models and algorithms to analyze the patterns and rules of transaction data and identify transaction behaviors that do not comply with the rules. Another method is to use graph theory and neural networks to analyze and study transaction flows and connection relationships in the blockchain network. By constructing transaction graphs and network maps, visualizing the relationships and connections between on-chain transaction data, identifying transaction flows, interaction patterns between addresses, and fund flow paths, abnormal nodes, transaction paths, and centralization can be discovered, thereby evaluating the security and stability of the blockchain network.

Abnormal Transaction Analysis and Detection Based on Data Mining and Machine Learning Currently, research on abnormal transaction analysis based on data mining and machine learning mainly focuses on deeply mining the features of blockchain node transaction data and discovering patterns and rules therein, so as to more effectively regulate the transaction behavior of blockchain networks. Zhu Huijuan et al. [80] proposed a blockchain abnormal transaction detection model, which adopts a residual network structure ResNet-32, and uses adaptive feature fusion methods to fully exploit the advantages of high-level abstract features and original features, improving the performance of blockchain abnormal transaction detection. This provides ideas for model construction and feature fusion for subsequent research. Taking the analysis of transaction motives as a starting point, Shen Meng et al. [81] designed a blockchain digital currency abnormal transaction behavior identification method based on motive analysis, selected airdrop candy and greedy funding as typical abnormal transaction behaviors, formulated judgment rules respectively, and abstracted abnormal transaction pattern diagrams, providing a reference for the classification and pattern research of abnormal transaction behaviors. Similarly, Zhang Xiaoqi et al. [82] proposed a network representation learning model DeepWalk-Ba for feature extraction of blockchain abnormal transactions. By constructing address and entity transaction graphs, combining features and machine learning for transaction entity identification, and extracting multi-granularity transaction patterns and user portraits based on transaction data analysis, timely and reliable detection of abnormal transactions in the blockchain can be achieved.

Abnormal Transaction Analysis and Detection Based on Graph Analysis and Neural Networks Wu et al. [83] designed two different community detection methods for Bitcoin and Ethereum networks, respectively proposing specific clustering algorithms derived from spectral clustering algorithms and novel community detection algorithms for low-level signals on graphs, helping to find user communities based on user token subscriptions. Further, Lin Wei [84] studied abnormal transaction data detection based on blockchain technology, and proposed a blockchain abnormal transaction data detection model based on a custom sliding window mechanism, a fully connected neural network, and a multi-channel output feature vector fusion of bidirectional gated recurrent units. In order to protect user privacy and reduce the risk of data being illegally obtained or abused during detection, Chen Binjie et al. [85] proposed a KNN-based blockchain abnormal transaction detection scheme with privacy protection. Accounting nodes randomize transaction data features by using matrix multiplication,

and then the cloud server uses KNN to detect abnormal transactions on the randomized transaction data features.

In terms of abnormal detection of smart contracts in blockchain, Liu et al. [86] proposed detecting fraudulent contracts by using transaction data and code data of Ethereum smart contracts, extracting features from complex smart contracts, effectively identifying abnormal contracts, and constructing a heterogeneous graph transformation network suitable for abnormal detection of smart contracts to detect financial fraud. However, whether more precise feature extraction methods can be developed to improve the efficiency of smart contract abnormal detection still needs further in-depth exploration.

2.1.2.2 Smart Contract Security Detection Smart contracts, as a core component of blockchain technology, have received much attention for their security issues. Research in this area is currently relatively mature [53, 87-90]. To ensure brevity, this section only briefly discusses relevant literature from a regulatory perspective.

Smart contract vulnerability detection methods include static analysis, dynamic analysis, formal verification, metamorphic testing, and graph neural network-based methods. These methods aim to identify potential vulnerabilities in smart contracts, such as reentrancy attacks, integer overflows, permission issues, and timestamp dependency issues. Since abnormal detection of smart contracts occurs before or after transactions and does not affect the final transaction results, this belongs to ex-ante or ex-post regulation.

1) Static Analysis By statically scanning and analyzing contract code, potential vulnerabilities are detected. Common tools include SmartCheck, Slither, etc.

2) Dynamic Analysis By simulating contract execution and monitoring its behavior, potential security issues can be found. ReGuard [91] generates random and diverse transaction data using fuzz testing, simulates possible attack scenarios, and dynamically identifies potential reentrancy attacks in smart contracts by recording key execution traces.

3) Formal Verification Verifies whether smart contracts comply with expected design attributes and security specifications. ZEUS [92] is an automated formal verification tool for smart contracts, which converts Solidity source code into LLVM (low-level virtual machine) intermediate language, and uses XACML (eXtensible access control markup language) to design five security vulnerability detection rules to determine the security of target programs during formal verification.

4) Metamorphic Testing By generating test cases and executing them in smart contracts, it verifies whether the test results meet expectations. In response to possible security vulnerabilities, Chen Jinfu et al. [93] designed different metamorphic relationships and performed metamorphic testing. By verifying whether the source test cases and subsequent test cases satisfy the metamorphic relationship, it determines whether there are related security vulnerabilities in the smart contract.

5) Deep Learning Based on the source code, operation code, and control flow patterns of smart contracts, features are extracted, and deep learning models (such as CNN, RNN, and Transformer) are used to train and predict whether there are security vulnerabilities. Deng et al. [94] proposed a smart contract vulnerability detection method using deep learning and multi-modal decision fusion, considering the code semantics and control structure information of smart contracts, and integrating source code, operation code, and control flow patterns through multi-modal decision fusion. Zhang et al. [95] proposed a hybrid deep learning model - convolutional and bidirectional gated recurrent unit (CBGRU), which combines word embedding methods (Word2Vec, FastText) and deep learning methods (LSTM, GRU, Bi-LSTM, CNN, BiGRU). Word embedding methods can convert words or phrases into vector representations to capture their semantic relationships. Different deep learning models extract smart contract features from different perspectives, combine them, and input them into a classifier for smart contract vulnerability detection.

Smart contract security is an important and complex field in blockchain technology. Many studies have been devoted to the detection and repair of smart contract security, but most vulnerability detection tools can only detect single and old versions of smart contract vulnerabilities [96]. Future research should focus on further improving the automation, efficiency, and accuracy of detection tools, combining static analysis methods with dynamic analysis methods to detect more types of vulnerabilities in multi-version smart contracts, thereby achieving higher detection accuracy.

2.1.2.3 Consensus Mechanism Attack Detection Consensus protocols are sets of rules in blockchain systems that determine transaction verification and block addition. Some common and harmful attacks include double-spending attacks, 51% attacks, selfish mining attacks, and saving attacks. Research on 51% attacks and double-spending attacks is relatively extensive and mature [97-100]. To ensure brevity, only saving attacks and selfish mining attacks, which have a greater impact on regulation, are briefly discussed.

Saving Attack is a new type of attack that can delay nodes from reaching consensus. Attackers "save" their proposed blocks during temporary consensus failures and use these rights to trigger another consensus failure after the network returns to normal, which leads to a decrease in blockchain performance and an increase in the delay of block finalization. Otsuki et al. [101] conducted a simulation study of Saving Attack on various fork selection rules, including the longest chain rule, GHOST (greedy heaviest-observed sub-tree), LMD GHOST (latest-message-driven GHOST), and FMD GHOST (fresh-message-driven GHOST). The research results show that Saving Attack has a very negative impact on consensus. Under experimental conditions, an attacker with 30% voting power successfully prevented LMD GHOST consensus for 83 minutes after saving their blocks for 32 minutes.

Selfish mining attacks are carried out by a small number of malicious miners or mining pools who exploit vulnerabilities or potential weaknesses in the system design to obtain more mining rewards unfairly. Wang et al. [102] used machine learning methods to detect selfish mining attacks in blockchain. They used logistic regression and fully connected neural networks (including 10 hidden layers and 10 neurons per layer) to train classification models on the training set, and judged whether unknown samples belonged to selfish mining attacks by learning the features of the samples, or belonged to ex-post regulation methods.

2.1.2.4 Consortium Chain Penetration Regulation Consortium chain penetration regulation is mainly located at the core function layer. Penetration regulation is a method introduced from the financial field into blockchain regulation, which refers to the regulation and traceability of all nodes and transaction data on the consortium chain through the penetration of regulatory nodes to ensure the security and stable operation of the consortium chain, and belongs to in-process regulation methods. In consortium chain regulation, regulatory logic can be embedded in the components of the core function layer, so penetration regulation can go deep into each entity for regulation and supervise and audit all transactions and information.

Liu Huixia et al. [103] proposed a blockchain-based security regulation scheme for shared charging piles, constructing a shared charging trust model based on a dual chain. They built a trust relationship between transaction parties through authentication contracts and designed a penetration regulation scheme to verify the identity of users, pile owners, or operators upwards, and verify the accuracy of charging amount, charging speed, and other information downwards, effectively regulating all participants and specific transaction data of car shared charging. Wang et al. [105] proposed an illegal data hierarchical interception scheme based on consortium chains. By using regular expressions and smart contracts at the application end to mark and block illegal data with different degrees of impact, it can effectively regulate illegal data in the blockchain. Different from previous single consortium chains, Zhang Jianyi et al. [106] adopted a regulable digital currency model with a consortium chain-public chain dual-chain structure, which uses the consortium chain as the core participant in consensus, ensures the privacy of user transaction data through secret sharing, and at the same time uses the public chain as the operating basis, allowing ordinary users to participate in and witness the maintenance of the system. In order to achieve comprehensive protection of transaction privacy and fine-grained mandatory regulation, Huo Xinlei et al. [107] proposed a consortium chain scheme with authorized regulation and privacy protection functions, including the division of member roles under the consortium chain and chameleon hash functions, zero-knowledge proofs, and other cryptographic technologies. Literature [106] focuses on the dual-chain structure and user participation, while literature [107] focuses on achieving comprehensive and fine-grained regulation and privacy protection through technical means.

In multiple application scenarios of consortium chains, researchers have also proposed some personalized solutions. In the field of agricultural machinery scheduling, Yang et al. [108] proposed a consortium blockchain-based agricultural machinery scheduling system. The upper-layer regulation improves the efficiency and security of the consensus algorithm and allows supervisors to block users with malicious intentions, ensuring the security of the system and improving the transparency and efficiency of data flow in the field of agricultural machinery scheduling. In the field of construction engineering, Li et al. [109] proposed the TABS (two-layer adaptive blockchain-based supervision) model for supervising off-site modular housing production, which realizes communication and transactions between adaptive private side chains and the main chain, ensuring the authenticity of operation records and protecting participant privacy, providing an unalterable and privacy-preserving regulatory mechanism for the construction engineering industry.

In addition, regulatory agencies can be considered as privileged nodes to access the consortium chain, and the effect of penetration regulation can be achieved by tracing and auditing on-chain data, which is a feasible regulatory direction.

In summary, core function layer regulation, in terms of abnormal transaction detection, researchers have proposed various methods to detect and analyze abnormal transactions on the blockchain, including abnormal transaction identification methods based on data mining and machine learning technologies, and using graph theory and neural networks to analyze and study transaction flows and connection relationships. Different studies have proposed various models and algorithms. For example, Zhu Huijuan et al. [80] used a residual network structure to improve detection

performance, while Zhang Xiaoqi et al. [82] performed transaction entity identification through network representation learning. Although these methods differ in technical details, their common goal is to improve the regulatory capabilities of blockchain networks and ensure the legality of transaction behavior. In terms of smart contract security detection, it can be seen that researchers refer to and learn from each other's work in abnormal transaction analysis and smart contract security. The static analysis, dynamic analysis, and formal verification methods mentioned in the literature complement each other and detect potential vulnerabilities in smart contracts from different angles. For example, formal verification methods verify whether smart contracts comply with design attributes, while dynamic analysis methods discover security issues by simulating smart contract execution. These studies are jointly committed to improving the security of smart contracts and reducing the risks brought by potential vulnerabilities. In terms of consortium chain regulation, in contrast to public chains, since regulation can be introduced as a basic function into the core function layer, or regulatory parties can be connected as nodes with regulatory authority, consortium chains can achieve penetration regulation.

2.1.3 User Layer Regulation

The user layer provides blockchain interfaces, blockchain nodes, user wallets, and other functions, supporting developers and miners to participate, use, and maintain the blockchain.

2.1.3.1 User Business Regulation User business regulation at the user layer mainly focuses on user business aspects, such as double-spending, false transactions, money laundering, Ponzi schemes, illegal token issuance, etc. Abnormal transaction behavior analysis and detection methods can be used to detect such businesses. Abnormal transaction behavior refers to the behavior of participants in a blockchain system that does not conform to normal transaction behavior patterns. In response to these abnormal transaction behaviors, the design and regulatory mechanisms of blockchain systems need to consider security and compliance, including identifying abnormal transaction behaviors, monitoring transaction patterns, and implementing compliance rules, etc., which are ex-post regulation methods, to reduce and prevent the occurrence of abnormal transaction behaviors. Related research focuses on abnormal transaction behaviors of blockchain users and corresponding regulatory mechanisms, which correspond to blockchain users and blockchain regulatory agencies, respectively.

Currently, blockchain abnormal transaction behavior identification methods have problems such as unclear identification targets, low efficiency in processing massive data, and single identification dimensions. In response to these problems, Zhao Zening [110] proposed an incremental identification method based on heuristic address clustering and a transaction behavior prediction method based on transaction subgraph partitioning, which improved the address clustering algorithm and improved the prediction accuracy by constructing transaction graphs and using graph neural networks. Qu Yuan [111] studied abnormal transaction behaviors in Bitcoin from two levels: macroscopic traffic data and microscopic transaction data. For macroscopic traffic data, unsupervised abnormal analysis and alarm functions were achieved by combining support vector machines and encoders and decoders. For microscopic transaction data, evolutionary graph convolutional networks (GCN) and time graph attention (TGA) mechanisms were used for feature extraction, and random forests were used for abnormal detection and alarming of illegal transactions, providing a more comprehensive abnormal detection solution. Existing solutions have improved identification accuracy, detection precision, and efficiency, but whether machine learning algorithms and encryption technologies can be combined to enhance the existing blockchain abnormal transaction behavior identification effect and privacy protection function still needs further in-depth exploration.

2.1.3.2 User Account Regulation Private keys are crucial for users to access their accounts and assets. Hackers may attack users' wallets, obtain private keys or tamper with transaction information by forging identities, inducing or deceiving users, thereby stealing assets. Ethereum has attracted a large number of users and developers, however, malicious users and attackers also use the anonymity and openness of Ethereum to engage in various illegal activities, such as pyramid schemes, fraud, money laundering, etc. Researchers have proposed machine learning, graph analysis, and time series analysis methods for Ethereum accounts to detect and identify malicious accounts, which belong to ex-ante or ex-post regulation methods.

In response to transaction security issues caused by fraudulent accounts in blockchain, Zhou Jian et al. [112] proposed a fraudulent account detection and feature analysis model based on machine learning, and introduced SHAP values to provide a more accurate prediction model through on-chain data feature analysis. Farrugia et al. [113] proposed a new method for detecting illicit users in Ethereum, which detects illicit activities on the Ethereum network at the account level by feature extraction and feature importance analysis, combined with the XGBoost classification model.

Liang Fei et al. [114-115] successively proposed methods based on hyperbolic graph neural convolutional networks (LSC-GCN) [114] and subspace graph clustering (GCN-Clustering) [115] to detect malicious Ethereum accounts. In response to the problems of insufficient labels in datasets leading to insufficient model training and low identification efficiency in existing models, GCN-Clustering converts original node address features into node features containing cluster

information, uses the clustering information of the dataset itself to enhance the feature extraction capability of nodes, and at the same time uses GCN for supervised learning, further strengthening the embedding expression of cluster information obtained in unsupervised learning in node features.

Shi Tuo et al. [116] incorporated transaction time information into the Ethereum address account feature model, proposed a graph attention mechanism based on time series transaction relationships, and improved the traditional attention network. By using the attention mechanism, the central node and neighboring nodes are aggregated, which can effectively identify Ethereum addresses with abnormal transaction behaviors.

For the wallet security of Bitcoin and three privacy-focused cryptocurrencies: Dash, Monero, and Zcash, Biryukov et al. [117] manually checked and used static analysis tools (such as FlowDroid, SmartDec Scanner) to scan and analyze wallets, detecting security threats in wallet installation methods, permission requirements, and privacy policies. They proposed a transaction clustering method based on transaction time analysis, listening to network traffic and attempting to associate attackers' cryptocurrency addresses with IP addresses or other identity information.

In summary, for the identification and regulation of abnormal behaviors (such as double-spending, false transactions, money laundering) in blockchain systems, researchers have proposed a series of methods based on heuristic address clustering, transaction subgraph partitioning, Ethereum Ponzi scheme detection, etc., aiming to improve the accuracy and efficiency of abnormal behavior identification. In addition, this section also focuses on account security and regulation issues, especially the theft of assets due to private key leakage. Existing research uses machine learning, graph analysis, and time series analysis methods to detect and identify malicious accounts and improve account security. With the continuous evolution of blockchain technology and the expansion of its application scope, future research can develop towards more refined abnormal behavior detection methods, more effective account security protection strategies, and more in-depth data analysis and mining technologies to adapt to increasingly complex and diverse security threats. At the same time, with the continuous improvement and strengthening of regulatory regulations, researchers also need to pay more attention to the compliance of blockchain systems to ensure their sustainable development and widespread application in business and finance.

Table 3 shows the comparison of blockchain regulatory technologies related to the infrastructure layer, core function layer, and user layer, where × indicates that it is not considered or is not the focus of the solution, and √ indicates that the solution is involved.

2.2 Inter-chain Regulation

Inter-chain regulation focuses on the interaction and interoperability regulation between different blockchains. The core services of inter-chain regulation are cross-chain asset exchange, inter-chain communication and data sharing, cross-chain App operations, smart contract interoperability, decentralized identity authentication, etc. There are two types of inter-chain regulation: one is to deploy regulatory logic on the regulatory chain based on the core idea of "governance by chain," where the regulated chain synchronizes data with the regulatory chain, and the regulatory chain can operate on the regulated chain; the other is to regulate existing cross-chain protocol

Table 3. Comparison of blockchain regulatory technologies

Section	Blockchain Monitoring Technology Comparison	Applicable	Monitoring Method	Network Security
Supervision Layer	Use ELK + Kafka + Fabric for transaction data trading monitoring	Fabric	Strong	✗
	Based on Kademlia protocol for node autonomous discovery	Public	Strong	✗
	Based on Ethereum/chain of blocks and the concept of account-based models of blockchain	Bitcoin	Strong	✗
	Node capability-based account structure model for blockchain transmission and method	Ethereum	Public	✗
	Use machine learning to predict abnormal node behavior based on network data	Bitcoin	Strong	✗
	Double spending attack detection based on Bitcoin trading data analysis (124)	Bitcoin	Strong	✗
Basic Infrastructure	Detection of nodes in the network and classify them, analyzing malicious nodes' behavior	Public	Medium	✓
	Ability to classify nodes based on node interaction behavior	Fabric	Weak	✗

	Based on GNX node classification, detect network nodes (123-125)	Ethereum	Strong	✗
	Use based on anomaly detection methods to study network nodes (126-127)	Ethereum	Strong	✗
	Use of KNN for network node classification	Public	Medium	✓
	Use of random forest for abnormal node detection based on the network environment	Ethereum	Strong	✗
Node Behavior Analysis & Detection Methods	Detect and analyze new abnormal behavior of nodes based on current network data (128)	Public	Medium	✗
	Based on signature and machine learning to detect new abnormal behaviors, such as DDoS attacks (134)	Public	Medium	✗
	Use of graph algorithms to analyze communication relationships between nodes (134)	Public	Medium	✗
	Use of deep learning to classify malicious behaviors, such as KNN for abnormal behavior detection (91)	Public	Medium	✓
Core Trust & Security	Automatic detection of trustworthiness based on behavior model (138)	Public	Medium	✗
	Construct local security models based on communication behaviors (92)	Public/Weak	Weak	✗
	Use abnormal behavior models for detection and prevention of malicious behaviors (90)	Public	Medium	✗
	Detect new malicious behavior patterns in blockchain communication (91)	Public	Medium	✗
Shared Mechanisms for Security	Use of simulations to analyze the impact of malicious behaviors on consensus (101)	POS	Strong	✗
	Use of replay attacks and attack simulation models to analyze malicious attacks (102)	Bitcoin	Strong	✗
	Construct-based security mechanism for shared liability and design trust protocols (103)	Ethereum	Strong	✗
	Role-based permission control based on security policies for secure access (104)	Ethereum	Medium	✓
Distributed Identity and User Management	Use of identity management and identity authentication based on blockchain (105)	POS	Strong	✗
	Use of blockchain for user identity management and privacy protection (106)	Bitcoin	Medium	✓
	User behavior tracking and account analysis based on user activity (107)	Ethereum	Weak	✗
	Use of LSC-GCN for GCN-Clustering methods to analyze user behaviors (113-116)	Ethereum	Strong	✗

2.2.1 Regulation Based on the "Governance by Chain" Concept Kevin Werbach et al. [119] first proposed the concept of "governance by chain" in the legal field. Chen Chun [57] further deepened this concept. The basic principle of "governance by chain" technology is to use one blockchain as a regulatory chain to regulate another blockchain, i.e., the regulated chain. The regulator can create a smart contract on the regulatory chain, which stipulates the rules and conditions to be complied with on the regulated chain. This leads to an important research direction - blockchain "compliance" regulation, which aims to ensure that blockchain transactions and activities comply with legal regulations, norms, and standards. These requirements can be any type of rule, such as transaction restrictions, prevention of double-spending, anti-money laundering, etc. When some nodes or users on the regulated chain violate these rules, the regulator can initiate sanctions on the regulatory chain through smart contracts. These sanctions usually involve penalties or disciplinary measures, such as freezing accounts, prohibiting transactions, or revoking transactions.

Ethereum, through ERC (Ethereum Request for Comments), standardizes smart contracts. From ERC20 to ERC1400, it has achieved a shift from avoiding regulation to embracing regulation [120]. ERC20 only requires providing functions such as token issuance and transfer, while ERC1400 stipulates the standard for issuing security tokens, requiring smart contracts to provide relevant legal documents and perform restriction judgments before executing transfers, providing readable explanations of judgment results, thereby realizing functions such as locking positions at the contract level, KYC/AML verification, and freezing in/out accounts. Libra also released White Paper 2.0 in 2020 to respond to regulatory concerns, including compliance controls (such as VASP certification, non-custodial wallet restrictions, etc.), making all transactions on the Libra blockchain enforce certain

compliance requirements. These measures are all aimed at improving the compliance and transparency of blockchain transactions and better adapting to regulatory requirements. Boya Zheng Chain provides a smart contract programming language RegLang [121] for regulatory technology. According to regulatory needs, it designs the syntax rules and type system of contracts. Regulators can automatically implement penetration regulation through smart contracts. Regulated objects can improve automated compliance capabilities through regulatory rules published by regulators, improving regulatory efficiency and accuracy, and making regulation more standardized, intelligent, and digital. Lu et al. [122] built the OriginChain system to provide transparent, tamper-proof, and traceable data, and automatically perform compliance checks. The system generates smart contracts representing legal agreements, automatically checks and executes services and terms, and checks whether legal and regulatory requirements are met. Mao Xiangke et al. [123] built a blockchain system with regulatory functions and rollback operations, realizing regulation of blockchain transactions at three different stages: pre-event, in-event, and post-event.

Some domestic enterprises are also actively promoting the implementation of "governance by chain" technology. Tencent Security released the "CCGP Cross-Chain Governance White Paper," realizing "governance by chain" cross-chain interoperability and collaboration. This system has five major advantages: strong universality, easy scalability, multi-party co-governance, high efficiency, high security, and traceable records, covering three application scenarios: wide-area data sharing, joint traceability, and wide-area evidence storage, which is expected to promote the application of blockchain technology in multiple scenarios. The Beijing Internet Court issued the "Tianping Chain" application access technology and management specifications [124], which standardize the technology and process of blockchain application access, improving the credibility and efficiency of electronic evidence. This specification involves three aspects: system security of the access platform, compliance of electronic data, and security of blockchain, promoting the application of blockchain technology in the judicial field. Literature [125-128] discusses smart contract compliance verification models in different application scenarios such as IoT, law, and cloud services, verifying and confirming the compliance of smart contracts in different environments.

Jing Pujie et al. [129] proposed a hierarchical cross-chain regulatory architecture based on the idea of "governance by chain," and designed a "regulatory chain-business chain" cross-chain collaborative governance model in the regulatory architecture, which improved the centralized and authoritarian nature of regulatory behavior. The designed cross-chain interaction standard data structure with universality ensures the smooth, secure, and efficient cross-chain regulatory process. Zhang et al. [130] proposed their on-chain hierarchical structure, on-chain and off-chain hybrid storage model, on-chain regulatory process, and traceable transaction information process. Through pre-event, in-event, and post-event collaborative regulation, multi-party hierarchical and multi-dimensional regulation of the entire data transaction process is achieved, and regulatory smart contracts are used to achieve hierarchical regulation of multiple regulators and post-event traceability (ex-post regulation), which can effectively isolate and protect sensitive information between data transactions.

2.2.2 Cross-chain Security Regulation Cross-chain technology is an important technical means to achieve inter-chain interconnection and value transfer. Cross-chain technology realizes interoperability and data exchange between different blockchains, but it also brings new security risks.

The security of cross-chain systems mainly depends on atomicity, inter-chain information synchronization, and network channel security. Given the diversity of heterogeneous blockchains in terms of block structure, consensus mechanisms, and complex working mechanisms, coupled with inherent security vulnerabilities in cross-chain technology, such as defects in the principles and implementation mechanisms of cross-chain technology, all these factors may cause security risks. In addition, if the consensus algorithm of the underlying blockchain has vulnerabilities or is compromised, the security of cross-chain interactive operations will also be threatened.

The notary mechanism may lead to collusion attacks and single point of failure risks. Notaries are nodes responsible for verifying and confirming cross-chain transactions. If notaries collude or a notary is attacked, the security of the entire cross-chain system will be threatened. The hash lock mechanism is a time-constrained mechanism used for cross-chain transactions, which may be affected by clock drift and malicious delay attacks. Clock drift may lead to inaccurate lock times, while malicious delay attacks exploit network delays to manipulate the execution order of cross-chain transactions. Wu Di [131] proposed defense methods against hash lock transfer delay attacks, relay cross-chain routing attacks, and relay chain block blocking attacks, which to a certain extent strengthened the security regulation of cross-chain systems. First, to prevent hash lock transfer delay attacks, the time difference can be increased. By increasing the time difference between the Fabric end and the ETH end, the difficulty for attackers to maliciously wait and block the network can be increased. Then, three protection methods can be adopted to deal with relay cross-chain routing attacks: application chain whitelist, application chain balance query, and application chain creation time query. Finally, by comprehensively using two methods: setting connection count scripts and modifying the

gateway's request processing order, relay chain block blocking attacks can be effectively prevented.

2.3 Off-chain Regulation

Off-chain regulation refers to regulators regulating and managing regulated chains through off-chain mechanisms, including community discussions, voting, negotiations, off-chain governance, committee decisions, and other methods. However, off-chain regulation has problems such as insufficient participation, abuse of power, and lack of transparency [132-133], which need to be solved through effective mechanisms and rules.

The Ethereum The DAO incident [134] and the Bitcoin block size debate [135] are two typical off-chain regulatory events. The Ethereum The DAO incident involved the security and governance issues of Ethereum smart contracts. Finally, the Ethereum community decided to hard fork the Ethereum blockchain through off-chain discussions and voting to recover stolen assets and maintain the stability of the Ethereum network. The Bitcoin block size debate lasted for several years, involving important matters such as Bitcoin network protocol updates and capacity expansion. However, the final decision was made by a few developers and miners through off-chain negotiations and voting, and most Bitcoin users did not participate in or understand this process. This lack of transparency and insufficient participation in regulation reflects some problems and limitations of off-chain regulation, and also triggers discussions and attempts at off-chain regulation. For example, the block node election protocol Whisk proposed by the Ethereum Open Research Forum Ethresearch was discussed and designed by multiple community members rather than official Ethereum personnel.

In practice, a combination of on-chain and off-chain regulation can achieve better regulatory and community governance effects. EOS [136] is a blockchain project based on the delegated proof of stake (DPoS) consensus algorithm, and its community governance mechanism adopts a combination of on-chain and off-chain regulation. Off-chain regulation includes community discussions, voting, and negotiations, while on-chain regulation is implemented through smart contracts. Miyachi et al. [137] proposed a modular hybrid privacy-preserving framework for enhancing medical information management, combining on-chain and off-chain regulation to design a reference model. It mainly realizes the interaction between on-chain and off-chain resources through a distributed software architecture, thereby realizing privacy management of different types of medical data.

3. FUTURE OUTLOOK OF BLOCKCHAIN REGULATION

From the analysis and summary of the three categories of blockchain regulatory technologies in Section 3, it can be seen that there are four common problems in current blockchain regulation.

1. Difficulty in Data Association Analysis Blockchain transaction data is stored in a distributed network. Due to the decentralization and anonymity of blockchain transactions, it is difficult for regulators to track the true identity of transaction participants. For example, on privacy public chains such as Monero, Dash, and Zcash, the identities of transaction participants and transaction details are not public, making it difficult for regulators to obtain complete transaction information, thereby making it difficult to discover and punish violations. It is difficult to regulate illegal transactions and behaviors in these blockchain networks.

A possible solution is to break through the association of chain group entities and anonymous digital identity recognition technologies, build a three-in-one associated regulation of blockchain entities-data-chain groups, and integrate machine learning to extract features of non-anonymous data such as network layer traffic data, and train targeted regulatory large language models. However, the security of the unique algorithms of large language models in blockchain security regulation also needs to be considered to ensure the security of the regulatory technology itself. A typical attack method against large language models is command injection. Attackers can construct inputs cleverly to make the model perform unexpected behaviors. If the blockchain regulatory interface based on large language models is abused, even with input specifications, attackers may still use command injection to exploit the authority of the regulatory interface, causing damage or interfering with the normal operation of the regulated blockchain application.

2.Insufficient Consideration of Business Compliance Regulation Existing regulatory schemes tend to use technical means to regulate a specific vulnerability or risk, ignoring the compliance and security risks of the regulatory target business itself, which may lead to regulatory loopholes. Existing regulatory methods and technologies [80-81, 84, 113] are generally less versatile. It should be considered to regulate on-chain business and security vulnerability risks collaboratively, and design specialized regulatory schemes or systems for business and technical risks respectively.

3.Low Cross-chain Collaboration Regulation Capability Blockchain cross-chain protocols have matured, and various cross-chain projects have emerged. Cross-chain is no longer limited to involving only two blockchains, but has evolved into complex cross-chain scenarios with multi-chain collaborative interconnection represented by

Polkadot. In this regard, corresponding blockchain regulatory research is not yet deep and sufficient. It is necessary to consider establishing cross-chain regulatory interoperability mechanisms [139] or multi-chain collaborative regulatory mechanisms, such as using Polkadot's parachain auction mechanism to embed regulatory logic into the obtained parachains, and regulating blockchain applications connected to the parachains.

4.High Regulatory Cost Since the operation of regulatory schemes or systems requires continuous external investment of resources, regulatory costs will only increase, and it is impossible to achieve self-sustaining regulation. For example, node detection and attack detection technologies require long-term maintenance of necessary network facilities or deployment of nodes to collect blockchain P2P layer traffic. Abnormal transaction analysis and smart contract security require a large amount of computing resources to train the necessary machine learning models to complete detection or identification. Node tracking technology requires a large amount of data analysis. Penetration regulation requires a large amount of software resources to meet regulatory requirements.

A possible way to balance regulatory costs is for blockchain regulators, as members of the blockchain community, to propose and vote on matters as members of decentralized autonomous organizations. The benefits generated by these processes can be used to reduce regulatory costs. Therefore, whether it is possible to quantify and model regulatory effectiveness and regulatory benefits using game theory based on the blockchain ecosystem model and regulatory costs, thereby further analyzing the specific role of regulation in the development of the blockchain ecosystem, is a direction that needs to be explored.

With the in-depth development of blockchain technology, various Rollup [140] projects aimed at solving the scalability problems of existing public chains have emerged, such as Arbitrum [141], Optimism [142], etc., as well as high-performance public chains adopting new accounting structures or sharding, such as Kaspa [143], Near [144], etc. The applicability of traditional regulatory technologies to them needs to be further tested. In addition, the emergence of decentralized exchanges has promoted the prosperity of the decentralized finance ecosystem, and the regulation of decentralized exchanges will be a key area of blockchain security regulation.

For the regulation of these emerging blockchain projects, feasible regulatory measures are as follows:

A. Regulation should consider using decentralized autonomous organizations to achieve regulation. For example, the decentralized communities of permissionless chains themselves have governance rights and voting rights for projects. These communities have low participation thresholds and are a major effective way of regulation.

B. The scope of regulation should be extended to various Rollup solutions and DeFi projects, and targeted regulation should be carried out according to their underlying implementation mechanisms, thereby increasing the coverage of regulation.

C. Attention should be paid to the new Bitcoin ecosystem and targeted regulation should be carried out. Recently, inscription ecosystems represented by Ordinals and Sats, rune ecosystems represented by Runes, and Bitcoin smart contract virtual machines have emerged. In the future, regulators should pay attention to these emerging blockchain projects.

4. CONCLUSION

The rapid development of blockchain has brought increasingly serious security issues, making blockchain security regulation a key research area. This paper analyzes and summarizes the current state of the blockchain ecosystem and briefly explains the domestic and international policy background of blockchain regulation. Based on the characteristics of current blockchain technology and its applications, it provides a three-layer division of intra-chain infrastructure, cross-chain expansion, and off-chain decentralized autonomous communities and applications. Based on this division, existing regulatory technologies and schemes are summarized and systematically analyzed and compared from three aspects: intra-chain regulation, inter-chain regulation, and off-chain regulation. The paper focuses on discussing relevant literature on infrastructure layer, core function layer, and user layer regulation within intra-chain regulation and compares their characteristics. It briefly discusses representative schemes for inter-chain and off-chain regulation, and finally summarizes and compares the three regulatory schemes: intra-chain, inter-chain, and off-chain. It also points out common problems in current blockchain security regulation, possible improvement directions, and emerging blockchain projects that regulators should pay attention to in the future.

REFERENCES

[1] CHOI T M, SIQIN T. Blockchain in logistics and production from blockchain 1.0 to blockchain 5.0: an intra-inter-organizational framework[J]. Transportation Research Part E: Logistics and Transportation Review, 2022, 160: 102653.

[2] ALIEF R N, PUTRA M A P, GOHIL A, et al. FLB2: layer 2 blockchain implementation scheme on federated learning technique[C]//Proceedings of the 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Piscataway: IEEE Press, 2023: 846-850.

[3] PIERRO G A, TONELLI R. Can solana be the solution to the blockchain scalability problem? [C]//Proceedings of the 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER). Piscataway: IEEE Press, 2022: 1219-1226.

[4] ROCKET T, YIN M F, SEKNIQI K, et al. Scalable and probabilistic leaderless BFT consensus through metastability[J]. arXiv Preprint, arXiv: 1906.08936, 2019.

[5] TANG Y, YAN J W, CHAKRABORTY C, et al. Hedera: a permissionless and scalable hybrid blockchain consensus algorithm in multiaccess edge computing for IoT[J]. IEEE Internet of Things Journal, 2023, 10(24): 21187-21202.

[6] FITZI M, WANG X C, KANNAN S, et al. Minotaur: multi-resource blockchain consensus[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2022: 1095-1108.

[7] JAYAPAL C, M J, S N R. An insight into NFTs, stablecoins and DEXs in blockchain[C]//Proceedings of the 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). Piscataway: IEEE Press, 2023: 1-6.

[8] DEVMANE M A. D-space: a decentralized social media app[C]//Proceedings of the 2023 2nd International Conference on Edge Computing and Applications (ICECAA). Piscataway: IEEE Press, 2023: 809-814.

[9] BREIKI H A. Trust evolution game in blockchain[C]//Proceedings of the 2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA). Piscataway: IEEE Press, 2022: 1-4.

[10] KARANJAI R, XU L, DIALLO N, et al. DeFaaS: decentralized function-as-a-service for emerging dApps and Web3[C]//Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Piscataway: IEEE Press, 2023: 1-3.

[11] GABRIEL T, CORNEL-CRISTIAN A, ARHIP-CALIN M, et al. Cloud storage. A comparison between centralized solutions versus decentralized cloud storage solutions using blockchain technology[C]//Proceedings of the 2019 54th International Universities Power Engineering Conference (UPEC). Piscataway: IEEE Press, 2019: 1-5.

[12] ZHONG Z S, WEI S R, XU Y T, et al. SilkViser: a visual explorer of blockchain-based cryptocurrency transaction data[C]//Proceedings of the 2020 IEEE Conference on Visual Analytics Science and Technology (VAST). Piscataway: IEEE Press, 2020: 95-106.

[13] SABLE N P, RATHOD V U, SABLE R, et al. The secure E-wallet powered by blockchain and distributed ledger technology[C]//Proceedings of the 2022 IEEE Pune Section International Conference (PuneCon). Piscataway: IEEE Press, 2022: 1-5.

[14] ARAB G A, COGLIATTI J I, URQUIZÓ P, et al. Development of a blockchain-based Web3 application for CO2 absortion right management[C]//Proceedings of the 2023 IEEE International Humanitarian Technology Conference (IHTC). Piscataway: IEEE Press, 2023: 1-4.

[15] CUI W P, SUN Y X, ZHOU J R, et al. Understanding the blockchain ecosystem with analysis of decentralized applications: an empirical study[C]//Proceedings of the 2021 the 5th International Conference on Management Engineering, Software Engineering and Service Sciences. New York: ACM Press, 2021: 38-44.

[16] SUN J, SADDIK A E, CAI W. Smart contract as a service: a paradigm of reusing smart contract in web3 ecosystem[J]. IEEE Consumer Electronics Magazine, 2024, 14(1): 46-55..

[17] RAIKWAR M, GLIGOROSKI D. Aggregation in blockchain ecosystem[C]//Proceedings of the 2021 Eighth International Conference on Software Defined Systems (SDS). Piscataway: IEEE Press, 2021: 138-143.

[18] DONG W L, LIU Z, LIU K, et al. Survey on vulnerability detection technology of smart contracts[J]. Journal of Software, 2024, 35(1): 38-62.

[19] WEI S J, LÜ W L, LI S S. Overview on typical security problems in public blockchain applications[J]. Journal of Software, 2022, 33(1): 324-355.

[20] HAN X, YUAN Y, WANG F Y. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1): 206-225.

[21] LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27.

[22] LIU A D, DU X H, WANG N, et al. Research progress on blockchain system security technology[J]. Chinese Journal of Computers, 2024, 47(3): 608-646.

[23] ZHOU S S, LI K, XIAO L J, et al. A systematic review of consensus mechanisms in blockchain[J]. Mathematics, 2023, 11(10): 2248.

[24] XU J, WANG C, JIA X H. A survey of blockchain consensus protocols[J]. ACM Computing Surveys, 2023, 55(13): 1-35.

[25] CHOO K R, OZCAN S, DEHGHANTANHA A, et al. Editorial: blockchain ecosystem: technological and management opportunities and challenges[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 982-987.

[26] KHANG A, CHOWDHURY S, SHARMA S. The data-driven blockchain ecosystem: fundamentals, applications, and emerging technologies[M]. Boca Raton: CRC Press, 2022.

[27] RIASANOW T, BURCKHARDT F, SETZKE D S, et al. The generic blockchain ecosystem and its strategic implications[C]//Proceedings of the 24th Americas Conference of Information Systems. Piscataway: IEEE Press, 2018. 1-10.

[28] REHMAN M H U, SALAH K, DAMIANI E, et al. Trust in blockchain cryptocurrency ecosystem[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1196-1212.

[29] STAFFORD T F, TREIBLMAIER H. Characteristics of a blockchain ecosystem for secure and sharable electronic medical records[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1340-1362.

[30] KABASHKIN I. Risk modelling of blockchain ecosystem[C]//International Conference on Network and System Security. Berlin: Springer, 2017: 59-70.

[31] YOO S. A study on blockchain ecosystem[J]. The Journal of the Institute of Webcasting, Internet and Telecommunication, 2018, 18: 1-9.

[32] KIM J W. Analysis of blockchain ecosystem and suggestions for improvement[J]. Journal of Information and Communication Convergence Engineering, 2021, 19(1): 8-15.

[33] RAIKWAR M, GLIGOROSKI D. DoS attacks on blockchain ecosystem[C]//European Conference on Parallel Processing. Berlin: Springer, 2022: 230-242.

[34] ZHANG H, YI J B, WANG Q. Research on the collaborative evolution of blockchain industry ecosystems in terms of value co-creation[J]. Sustainability, 2021, 13(21): 11567.

[35] PAPADONIKOLAKI E, TEZEL A, YITMEN I, et al. Blockchain innovation ecosystems orchestration in construction[J]. Industrial Management & Data Systems, 2023, 123(2): 672-694.

[36] ZHANG W, DONG W, ZHANG F Q, et al. The application of German blockchain technology in the field of financial science and technology, its supervision ideas and its enlightenment to China[J]. International Finance, 2019(9): 76-80.

[37] YANG D, CHEN Z L. Virtual currency legislation: experience of Japan and inspiration to China[J]. Securities Market Herald, 2018(2): 69-78.

[39] DENG J P. Blockchain regulatory mechanism and enlightenment in United States[J]. China Policy Review, 2019(1): 125-130.

[40] DENG J P. Singapore's blockchain regulatory policy and its review[J]. Fudan University Law Review, 2020(1): 59-72.

[41] PI L Y, XUE Z W. Regulation arrangement and international practice of crypto-asset transactions[J]. Securities Market Herald, 2019(7): 4-12.

[45] LIU H Q, RUAN N. A survey on attacking strategies in blockchain[J]. Chinese Journal of Computers, 2021, 44(4): 786-805.

[46] YU G, NIE T Z, LI X H, et al. The challenge and prospect of distributed data management techniques in blockchain systems[J]. Chinese Journal of Computers, 2021, 44(1): 28-54.

[47] XU K, LING S T, LI Q, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 55-83.

[48] QIN C X, GUO B, SHEN Y, et al. Security risk assessment model of blockchain[J]. Acta Electronica Sinica, 2021, 49(1): 117-124.

[49] QIAN P, LIU Z G, HE Q M, et al. Smart contract vulnerability detection technique: a survey[J]. Journal of Software, 2022, 33(8): 3059-3085.

[50] CUI Z Q, YANG H W, CHEN X, et al. Research progress of security vulnerability detection of smart contracts[J]. Journal of Software, 2024, 35(5): 2235-2267.

[51] JIANG F, CHAO K L, XIAO J M, et al. Enhancing smart-contract security through machine learning: a survey of approaches and techniques[J]. Electronics, 2023, 12(9): 2046.

[52] WU H G, PENG Y B, HE Y Q, et al. A review of deep learning-based vulnerability detection tools for Ethernet smart contracts[J]. Computer Modeling in Engineering & Sciences, 2024, 140(1): 77-108.

[53] CHU H T, ZHANG P C, DONG H, et al. A survey on smart contract vulnerabilities: data sources, detection and repair[J]. Information and Software Technology, 2023, 159: 107221.

[54] CHEN J F, FENG Q W, CAI S H, et al. Vulnerability detection model for blockchain systems based on formal method[J]. Journal of Software, 2024, 35(9): 4193-4217.

[55] WANG Y, GOU G P, LIU C, et al. Survey of security supervision on blockchain from the perspective of technology[J]. Journal of Information Security and Applications, 2021, 60: 102859.

[56] YE C C, LI G Q, CAI H M, et al. Security detection model of blockchain[J]. Journal of Software, 2018, 29(5): 1348-1359.

[57] CHEN C. Key technologies of consortium blockchain and regulatory challenges of blockchain[R]. 2019.

[58] MÖSER M, BÖHME R, BREUKER D. Towards risk scoring of Bitcoin transactions[C]//Financial Cryptography and Data Security. Berlin: Springer, 2014: 16-32.

[59] ANDERSON R. Making Bitcoin legal (transcript of discussion) [C]//Security Protocols XXVI. Berlin: Springer, 2018: 254-265.

[60] TOVANICH N, CAZABET R. Pattern analysis of money flows in the Bitcoin blockchain[C]//International Conference on Complex Networks and Their Applications. Berlin: Springer, 2023: 443-455.

[61] LI Z Y, XU B L, ZHOU Y Y. Blockchain anonymous transaction tracking method based on node influence[J]. Computer Science, 2024, 51(7): 422-429.

[62] LI S S, WANG Y Z, ZOU Y L, et al. Consensus transaction trajectory visualization tracking method for Fabric based on custom logs[J]. Journal of Computer Applications, 2022, 42(11): 3421-3428.

[63] ZHENG L W, HELU X H, LI M H, et al. Automatic discovery mechanism of blockchain nodes based on the kademlia algorithm[C]//International Conference on Artificial Intelligence and Security. Berlin: Springer, 2019: 605-616.

[64] MICHALSKI R, DZIUBAŁTOWSKA D, MACEK P. Revealing the character of nodes in a blockchain with supervised learning[J]. IEEE Access, 2020, 8: 109639-109647.

[65] GOMEZ G, MORENO-SANCHEZ P, CABALLERO J. Watch your back: identifying cybercrime financial relationships in Bitcoin through back-and-forth exploration[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2022: 1291-1305.

[66] DU H B, CHE Z, SHEN M, et al. Breaking the anonymity of ethereum mixing services using graph feature learning[J].

IEEE Transactions on Information Forensics and Security, 2024, 19: 616-631.

[67] LIN D K, YAN J Q, LANDENG B, et al. Survey of anonymity and tracking technology in monero[J]. Journal of Computer Applications, 2022, 42(1): 148-156.

[68] FU Z H, LIN D K, JIANG H C, et al. Survey of anonymous and tracking technology in zerocash[J]. Computer Science, 2021, 48(11): 62-71.

[69] KUMAR A, FISCHER C, TOPLE S, et al. A traceability analysis of monero's blockchain[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2017: 153-173.

[70] LIU G Z. Research and implementation of abnormal traffic monitoring method based on federated learning[D]. Beijing: Beijing University of Posts and Telecommunications, 2021.

[71] SANDA O, PAVLIDIS M, SERAJ S, et al. Long-range attack detection on permissionless blockchains using deep learning[J]. Expert Systems with Applications, 2023, 218: 119606.

[72] ZHANG Z, HE T, CHEN K, et al. Phishing node detection in ethereum transaction network using graph convolutional networks[J]. Applied Sciences, 2023, 13(11): 6430.

[73] YU T, CHEN X M, XU Z, et al. MP-GCN: a phishing nodes detection approach via graph convolution network for ethereum[J]. Applied Sciences, 2022.

[74] DAI Q Y, ZHANG B, DONG S Q. Eclipse attack detection for blockchain network layer based on deep feature extraction[J]. Wireless Communications and Mobile Computing, 2022, 2022(1): 1451813.

[75] DAI Q Y, ZHANG B, XU K Y, et al. An Erebus attack detection method oriented to blockchain network layer[J]. Computers, Materials & Continua, 2023, 75(3): 5395-5431.

[76] DAI Q Y, ZHANG B, DONG S Q. A DDoS-attack detection method oriented to the blockchain network layer[J]. Security and Communication Networks, 2022, 2022: 5692820.

[77] LYU J S, YANG P, CHEN W, et al. Abnormal detection of eclipse attacks on blockchain based on immunity[J]. Computer Science, 2018, 45(2): 8-14.

[78] ALANGOT B, REIJSBERGEN D, VENUGOPALAN S, et al. Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1659-1672.

[79] CAO W(J/Q). Research on detection method of trusted link flooding attack based on blockchain[D]. Hefei: University of Science and Technology of China, 2022.

[80] ZHU H J, CHEN J F, LI Z Y, et al. Block-chain abnormal transaction detection method based on adaptive multi-feature fusion[J]. Journal on Communications, 2021, 42(5): 41-50.

[81] SHEN M, SANG A Q, ZHU L H, et al. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency[J]. Chinese Journal of Computers, 2021, 44(1): 193-208.

[82] ZHANG X Q, BAI X, LI G S, et al. Blockchain abnormal transaction detection based on network representation learning[J]. Cyber Security and Data Governance, 2022, 41(10): 11-20.

[83] WU S X, WU Z X, CHEN S H, et al. Community detection in blockchain social networks[J]. Journal of Communications and Information Networks, 2021, 6(1): 59-71.

[84] LIN W. Detection of abnormal transactions in blockchain based on multi feature fusion[J]. Netinfo Security, 2022(10): 24-30.

[85] CHEN B J, WEI F S, GU C X. Blockchain abnormal transaction detection with privacy-preserving based on KNN[J]. Netinfo Security, 2022, 22(3): 78-84.

[86] LIU L, TSAI W T, BHUIYAN M Z A, et al. Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum[J]. Future Generation Computer Systems, 2022, 128: 158-166.

[87] HE D J, DENG Z, ZHANG Y X, et al. Smart contract vulnerability analysis and security audit[J]. IEEE Network, 2020, 34(5): 276-282.

[88] VACCA A, SORBO A D, VISAGGIO C A, et al. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges[J]. Journal of Systems and Software, 2021, 174: 110891.

[89] CHEN H S, PENDLETON M, NJILLA L, et al. A survey on ethereum systems security: vulnerabilities, attacks, and defenses[J]. ACM Computing Surveys, 2020, 53(3): 1-43.

[90] KANNENGIEßER N, LINS S, SANDER C, et al. Challenges and common solutions in smart contract development[J]. IEEE Transactions on Software Engineering, 2022, 48(11): 4291-4318.

[91] LIU C, LIU H, CAO Z, et al. ReGuard: finding reentrancy bugs in smart contracts[C]//Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings. New York: ACM Press, 2018: 65-68.

[92] KALRA S, GOEL S, DHAWAN M, et al. ZEUS: analyzing safety of smart contracts[C]//Proceedings 2018 Network and Distributed System Security Symposium. Piscataway: IEEE Press, 2018: 1-12.

[93] CHEN J F, WANG Z X, CAI S H, et al. Vulnerability detection method for blockchain smart contracts based on metamorphic testing[J]. Journal on Communications, 2023, 44(10): 164-176.

[94] DENG W C, WEI H C, HUANG T, et al. Smart contract vulnerability detection based on deep learning and multimodal decision fusion[J]. Sensors, 2023, 23(16): 7246.

[95] ZHANG L J, CHEN W J, WANG W Z, et al. CBGRU: a detection method of smart contract vulnerability based on a hybrid model[J]. Sensors, 2022, 22(9): 3577.

[96] HE D J, WU R, LI X J, et al. Detection of vulnerabilities of blockchain smart contracts[J]. IEEE Internet of Things Journal, 2023, 10(14): 12178-12185.

[97] RAMEZAN G, LEUNG C. Analysis of proof-of-work-based blockchains under an adaptive double-spend attack[J]. IEEE Transactions on Industrial Informatics, 2020, 16(11): 7035-7045.

[98] ZHENG J, HUANG H W, ZHENG Z B, et al. Adaptive double-spending attacks on PoW-based blockchains[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(3): 1098-1110.

[99] SAAD M, SPAULDING J, NJILLA L, et al. Exploring the attack surface of blockchain: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1977-2008.

[100] CHULERTTIYAWONG D, JAMALIPOUR A. Sybil attack detection in Internet of flying things-IoFT: a machine learning approach[J]. IEEE Internet of Things Journal, 2023, 10(14): 12854-12866.

[101] OTSUKI K, NAKAMURA R, SHUDO K. Impact of saving attacks on blockchain consensus[J]. IEEE Access, 2021, 9: 133011-133022.

[102] WANG Z J, LV Q Z, LU Z B, et al. ForkDec: accurate detection for selfish mining attacks[J]. Security and Communication Networks, 2021, 2021(1): 5959698.

[103] LIU H X, LI L L. Security supervision scheme of shared charging pile based on blockchain[J]. Application Research of Computers, 2022, 39(5): 1319-1323, 1348.

[105] WANG X Q, ZHANG K, DING Y, et al. An illegal data supervision scheme for the consortium blockchain[C]//Blockchain Technology and Application. Berlin: Springer, 2022: 100-115.

[106] ZHANG J Y, WANG Z Q, XU Z L, et al. A regulatable digital currency model based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(10): 2219-2232.

[107] HUO X L, LONG Y, GU D W. Privacy protection and authorization supervision scheme based on consortium chain[J]. Journal of Chinese Computer Systems, 2023, 44(3): 589-595.

[108] YANG H T, XIONG S M, FRIMPONG S A, et al. A consortium blockchain-based agricultural machinery scheduling system[J]. Sensors, 2020, 20(9): 2643.

[109] LI X, WU L, ZHAO R, et al. Two-layer adaptive blockchain-based supervision model for off-site modular housing production[J]. Computers in Industry, 2021, 128: 103437.

[110] ZHAO Z N. Research on key technologies of blockchain abnormal trading behavior identification[D]. Tianjin: Tianjin University of Technology, 2023.

[111] QU Y. Research and design of Bitcoin abnormal behavior detection system[D]. Chengdu: University of Electronic Science and Technology of China, 2021.

[112] ZHOU J, ZHANG J, YAN S. Research on blockchain fraud account detection based on data on chain[J]. Application Research of Computers, 2022, 39(4): 992-997.

[113] FARRUGIA S, ELLUL J, AZZOPARDI G. Detection of illicit accounts over the ethereum blockchain[J]. Expert Systems with Applications, 2020, 150: 113318.

[114] LIANG F, WEI L, LIN W C. A method for detecting malicious Ethereum accounts based on subspace graph clustering [J]. Journal of Information Security Research, 2023, 9(E1): 68-71.

[115] LIANG F, MA L, ZHAI B Y, et al. Detection of malicious accounts in ethereum based on hyperbolic space graph neural convolution network[J]. Civil-Military Integration on Cyberspace, 2022(9): 48-52.

[116] SHI T, LIANG F, SHANG G C, et al. Detection of malicious ethereum account based on time series transaction and graph attention neural network[J]. Netinfo Security, 2022, 22(10): 69-75.

[117] BIRYUKOV A, TIKHOMIROV S. Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash[J]. Pervasive and Mobile Computing, 2019, 59: 101030.

[118] XU W K. Node detection algorithm for preventing blockchain bifurcation[J]. Electronic Technology & Software Engineering, 2020(3): 186-187.

[119] WERBACH K, LIN S W. Trust, but verify: why the blockchain needs the law[J]. Oriental Law, 2018(4): 83-115.

[120] KONG H D. Study on the legal nature of non-homogeneous general certificate[J]. Network Security Technology & Application, 2022(9): 141-143.

[121] GAO J B, ZHANG J S, LI Q S, et al. RegLang: a smart contract programming language for regulation[J]. Computer Science, 2022, 49(6): 462-468.

[122] LU Q H, XU X W. Adaptable blockchain-based systems: a case study for product traceability[J]. IEEE Software, 2017, 34(6): 21-27.

[123] MAO X K, LI C, HAO Y T, et al. A blockchain system design and implementation for all-round supervision[J]. Computer & Digital Engineering, 2023, 51(1): 81-85, 92.

[124] ZHANG Y N, WU P C. The construction of “balance chain” in Beijing Internet court and its enlightenment: also on the feasibility of blockchain technology to maintain the authenticity of electronic files[J]. Archives & Construction, 2022(10): 63-65.

[125] AMATO F, COZZOLINO G, MOSCATO F, et al. A model for verification and validation of law compliance of smart contracts in IoT environment[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7752-7759.

[126] PARVIZIMOSAED A, SHARIFI S, AMYOT D, et al. Subcontracting, assignment, and substitution for legal contracts in symboleo[C]//Conceptual Modeling. Berlin: Springer, 2020: 271-285.

[127] MOLINA-JIMENEZ C, SFYRAKIS I, SOLAIMAN E, et al. Implementation of smart contracts using hybrid architectures with on and off-blockchain components[C]//Proceedings of the 2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2). Piscataway: IEEE Press, 2018: 83-90.

[128] PARVIZIMOSAED A, BASHARI M, KIAN A R, et al. Compliance checking for transactive energy contracts using smart contracts[C]//Proceedings of the 2020 IEEE PES Transactive Energy Systems Conference (TESC). Piscataway: IEEE Press, 2020: 1-5.

[130] ZHANG Y Q, MA Z F, LUO S S, et al. DBSDS: a dual-blockchain security data sharing model with supervision and privacy-protection[J]. Concurrency and Computation: Practice and Experience, 2023, 35(21): e7706.

[131] WU D. Research on multi-scenario attack and defense method for cross-chain system[D]. Beijing: Beijing Jiaotong University, 2022.

[132] BRINKMANN M, HEINE M. Can blockchain leverage for new public governance: a conceptual analysis on process level[C]//Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance. New York: ACM Press, 2019: 338-341.

[133] DURSUN T, ÜSTÜNDAĞ B B. A novel framework for policy based on-chain governance of blockchain networks[J]. Information Processing & Management, 2021, 58(4): 102556.

[134] DIROSE S, MANSOURI M. Comparison and analysis of governance mechanisms employed by blockchain-based distributed autonomous organizations[C]//Proceedings of the 2018 13th Annual Conference on System of Systems Engineering (SoSE). Piscataway: IEEE Press, 2018: 195-202.

[135] USHIDA R, ANGEL J. Regulatory considerations on centralized aspects of DeFi managed by DAOs[C]//Financial Cryptography and Data Security. Berlin: Springer, 2021: 21-36.

[136] MONCADA R, FERRO E, FAVENZA A, et al. Next generation blockchain-based financial services[C]//Euro-Par 2020: Parallel Processing Workshops. Berlin: Springer, 2021: 30-41.

[137] MIYACHI K, MACKEY T K. hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design[J]. Information Processing & Management, 2021, 58(3): 102535.

[138] BARATI M, RANA O. Tracking GDPR compliance in cloud-based service delivery[J]. IEEE Transactions on Services Computing, 2022, 15(3): 1498-1511.

[139] YANG D. “Rule of law by chain” and “Chain-based governance”: the integration path of blockchain technology regulation [R]. 2019.

[140] GORZNY J, LIN P A, DERKA M. Ideal properties of rollup escape hatches[C]//Proceedings of the 3rd International Workshop on Distributed Infrastructure for the Common Good. New York: ACM Press, 2022: 7-12.

[141] KALODNER H A, GOLDFEDER S, CHEN X Q, et al. Arbitrum: scalable, private smart contracts[C]//27th USENIX Security Symposium. Berkeley: USENIX Association, 2018: 1353-1370.

[142] GONÇALVES J P D B, VILLAÇA R D S. A new consensus mechanism for blockchained federated learning systems using optimistic rollups[C]//Proceedings of the 2024 IEEE International Conference on Blockchain. Piscataway: IEEE Press, 2024: 406-411.

[143] SOMPOLINSKY Y, WYBORSKI S, ZOHAR A. PHANTOM GHOSTDAG: a scalable generalization of nakamoto consensus: September 2, 2021[C]//Proceedings of the 3rd ACM Conference on Advances in Financial Technologies. New York: ACM Press, 2021: 57-70.

[144] SNEHLATA, SHUKLA P, SINGH A K, et al. An intelligent blockchain-oriented digital voting system using NEAR protocol[J]. SN Computer Science, 2023, 4(5): 643.

[145] Aloun, M. S. (2024). Synergistic Integration of Artificial Intelligence and Blockchain Technology: Advancements, Applications, and Future Directions. Journal of Intelligent Systems and Applied Data Science, 2(2).