A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology

1st Pengxu Shen
School of Cyberspace Security
Hainan University
Haikou, China
21210839000019@hainanu.edu.cn

2nd Suozai Li
China Electronics Corporation
Hainan Joint Innovation Research Institute Co. Ltd
Chengmai, China
lisuozai@jiri.ac.cn

3rd Ming Huang
China Electronics Corporation
Hainan Joint Innovation Research Institute Co. Ltd
Chengmai, China
huangming@jiri.ac.cn

4th Haoyu Gao
College of Data Science and Application
Inner Mongolia University of Technology
Hohhot, China
20191800498@imut.edu.cn

5th Leixiao Li
College of Data Science and Application
Inner Mongolia University of Technology
Hohhot, China
llxhappy@126.com

6th Jun Li
School of Cyberspace Security
Hainan University
Oxford-Hainan Blockchain Research Institute
Chengmai, China
junli@hainanu.edu.cn

7th Hong Lei
School of Cyberspace Security
Hainan University
SSC Holding Company Ltd
Chengmai, China
leiluono1@163.com

2022 IEEE International Conference on Blockchain (Blockchain) | 978-1-6654-6104-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/BLOCKCHAIN55522.2022.00076

***Abstract*—Blockchain's technological characteristics, such as decentralization, robustness, and anti-modification, represent a significant challenge to the regulation of existing networks and data security. Effective regulation of blockchain applications is one of the keys to maintain the healthy and sustainable development of the blockchain ecology. We analyze the merits and demerits of the existing technologies in the research directions of tracking and visualization of blockchain nodes, consortium blockchain penetration regulation technology, public chain active discovery and exploration disposition techniques, and chain governance. In the end, we present the future research directions in respect of blockchain traceability and compliance regulation.**

***Keywords*—blockchain ecology, regulatory technology, blockchain traceability, compliance regulation**

I. Introduction

The innovative combination of blockchain technology and multidisciplinary research results has provided opportunities for change in many industries. However, in the process of rapid blockchain development, the lack of corresponding effective regulatory technology has led to frequent security incidents such as illegal money laundering, fraud and terrorist financing, among which the typical ones are Silk Road, Rug pull scam and Islamic State terrorist financing. As shown in Fig.1, the losses caused by blockchain security incidents have reached $6 billion in 2019 alone and even $10 billion in 2021[1]. In response to this phenomenon, many scholars have proposed blockchain regulation, such as regulating blockchain applications and their ecology through appropriate regulatory techniques. Compared with the regulatory model of other industries, blockchain regulation faces more difficulties. For example, the information security regulation of cloud computing can be accomplished through a centralized institution, a unified and efficient regulatory system and an effective industry self-regulatory mechanism at the national level. In contrast, the decentralized nature of blockchain must be achieved through blockchain traceability and compliance regulation, which fundamentally eliminates the involvement of a centralized institution.

In 2019, Chen et al.[2] put forward four major directions of current blockchain regulation technology when discussing the key technologies of coalition blockchain and the regulatory challenges of blockchain:

- Tracking and visualization of blockchain nodes.
- Consortium blockchain penetration regulation technology.
- Public chain active discovery and exploration disposition techniques.
- Chain governance.

Besides, effective coordination of data privacy security issues and regulatory issues for users on blockchain nodes will also be the focus of our future discussions.

We contributed mainly to the following:

This work was supported in part by the National Key R&D Program of China (No.2021YFB2700601); in part by the Finance Science and Technology Project of Hainan Province (No.ZDKJ2020009); in part by the National Natural Science Foundation of China (Nos. 62163011).

978-1-6654-6104-7/22/$31.00 ©2022 IEEE
DOI 10.1109/Blockchain55522.2022.00076

- We summarize the advantages and disadvantages of current regulatory technologies in terms of blockchain transaction data and behavior analysis, and the underlying blockchain compliance rules.
- Based on the four major research directions of blockchain regulatory technology, we propose relevant research ideas for compliance regulation and blockchain traceability.
- For blockchain regulation, in the future, we envision that a regulable model can be constructed and integrated into the blockchain system to realize the supervision and traceability of data information in the blockchain within the system.

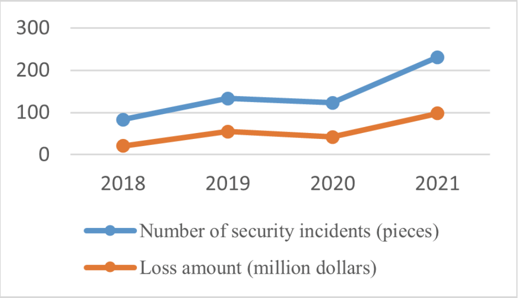

Fig. 1. Blockchain security incidents and loss amounts from 2018 to 2021.

The rest of the paper is organized as follows: in Section 1, we introduce the background and concepts of blockchain regulation and briefly propose the current research directions of regulatory technologies. In Section 2, we analyze the impact of blockchain decentralization, robustness and anti-modification features on blockchain regulation. In Section 3, we introduce the four mainly directions of the current blockchain regulatory technology development, from which we analyze the advantages and disadvantages of the existing technologies. In Section 4, we summarize the advantages and disadvantages of current regulatory technologies, and propose future research directions from both blockchain traceability and compliance regulation.

II. Blockchain Technology Features

The core features of blockchain are mainly embodied in technologies such as peer-to-peer networks, asymmetric encryption, and consensus mechanisms, which are decentralization, robustness and anti-modification, and can store data in a public, non-repudiation, and anonymous manner. While these features make blockchain a new and efficient tool to drive economic and social activities, they also make us realize that traditional regulatory tools cannot effectively regulate blockchain.

A. Decentralization

Blockchain, due to the absence of a centralized institution or gatekeeper, leads to the fact that anyone can download the appropriate software and examine the information stored on the chain[3]. Some of the new services can be used directly through the blockchain to perform actions such as information storage, value transfer, or coordination of social and economic activities. The decentralization of blockchain also exhibits a certain degree of de-legalization[8], making it free from existing rules and legal regulations and creating opportunities for illegal activities.

B. Robustness and Anti-modification

The robustness of blockchain ensures that it is difficult to close or delete the blockchain. Based on the tamper-proof technical characteristics of blockchain, it is difficult to delete or rollback information once it is written into the blockchain, especially the deployment of smart contracts, which is likely to facilitate illegal organizations in case of loopholes. These features are beneficial to the blockchain to maintain the status quo, but they also make it difficult to update the blockchain infrastructure.

C. Transparent and Non-repudiation

Peer-to-peer networks ensure the openness of data on the blockchain. Except for some specific encrypted information, participants on the blockchain have public access to information about transactions in which the account is involved and records of interactions with smart contracts. Digital signatures can be used as evidence to ensure the non-repudiation of data[3]. In a blockchain network, whether a user is posting a message or verifying its authenticity, the blockchain is proving the integrity of the message and the authenticity of the source in a non-repudiation way. The transparent and non-repudiation of blockchain, together with its robustness and anti-modification characteristics, make people convinced that the information on blockchain cannot be modified in the future or in the past. This means that malicious information will always be stored in the blockchain, bringing security risks to national and social governance.

D. Anonymity

Through asymmetric cryptography and digital signatures, users are active in the blockchain network with an anonymous identity, which makes certain organizations wandering in the gray areas of society use blockchain for illegal social activities and economic transactions[4][5]. Some Blockchains hide the real identity of users by using advanced cryptographic techniques such as zero-knowledge proofs and ring signatures to hide transaction information in the blockchain network, such as Zcash and Monroe[6]. If obfuscation and anonymity techniques are widely used, the regulatory difficulty of blockchain networks will further increase.

III. Current Regulatory Technologies

A. Tracking and Visualization of Blockchain Nodes

As shown in Fig.2, by investigating and analyzing the network addresses, account addresses and transactions of each node in the blockchain, we construct a “graph” of all nodes using dynamic visualization to show the network addresses, account addresses and transaction information of

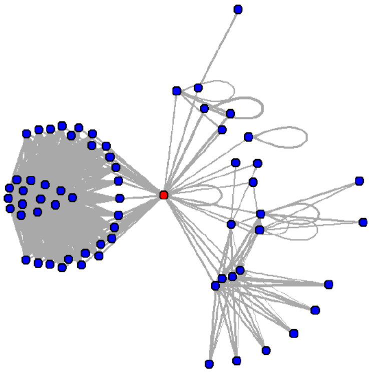

Fig. 2. A graph of the BTC transaction network.

each node, which facilitates managers to effectively manage the participants of the blockchain. The research on blockchain node tracking and visualization has shifted from showing the topology of the whole blockchain network through the list of IP addresses of blockchain nodes to discovering more behavioral characteristics through the analysis of blockchain transaction data.

Shen et al.[7] proposed a method to identify abnormal trading behavior of blockchain digital currencies based on motivation analysis. By designing the corresponding determination rules for two typical types of abnormal trading behaviors, namely, airdrop candy and greedy injection, the identification of these two types of abnormal bitcoin trading behaviors is achieved by using a subgraph matching algorithm. Based on this method, the administrator can discover the address groups with abnormal transaction behaviors in a short time and make corresponding solutions. Zheng et al.[8] proposed an automatic node discovery mechanism based on the Kademila protocol. The routing table composed by the Kademila protocol can cause the nodes in the network to be discovered by a node, and these nodes can be gradually added to that node, and the node's awareness of the dynamics of the entire network allows each node in the network to achieve data consistency at some point, and also provides for the automatic discovery of blockchain nodes. In contrast to research aimed at detecting Ponzi schemes disguised as smart contracts, anomalous transactions related to illegal activities, and money laundering schemes, Steven et al.[9] propose a new method to detect illegal users of Ether at the “account level” through feature extraction and feature importance by using XGBoost classification model is used to detect illegal activities on the ethereum network at the account level, and the effectiveness of the model is experimentally demonstrated.

Blockchain node tracking and visualization techniques are still mainly divided into two categories: one is to filter out address clusters or nodes with abnormal behaviors by performing data analysis and feature extraction operations on existing transaction data. The other is to visualize the blockchain by sensing the dynamics of the whole blockchain network through the routing table in the blockchain nodes via relevant protocols. The former can get more ideal results through data analysis for anomalous behaviors with defined detection rules. However, once new anomalous behaviors appear, it is necessary to organize new transaction data sets and redesign detection algorithms.

B. Consortium Blockchain Penetration Regulation Technology

Unlike the decentralization of the public chain, the federation to some extent only belongs to the internal members of the federation and presents the characteristic of partial decentralization. Moreover, due to the limited number of nodes in the consortium blockchain, it is easier to reach consensus, more efficient operation and higher controllability compared with the public chain. The data is only open to consortium members, and the non consortium members cannot access the data inside the consortium blockchain, and the data between different businesses are also isolated to a certain extent, which has better privacy protection.

The concept of penetrating regulation originates from finance, which is to see through the surface form of financial products to the substance of financial business and behavior, and to adopt relevant strategies to implement whole-process regulation of financial institutions' business and behavior according to the principle of ”substance over form”. In the consortium blockchain, the penetrating regulation is to regulate the essence of various behaviors of all parties involved in the chain, mainly in terms of functions and behaviors.

Wang et al.[10] proposed a scheme to determine users' resource access and usage rights by means of anonymous certificates based on the regulatory issues arising from the anonymous authentication process. The user can selectively present attributes when presenting the certificate to ensure that the user's private information is not over-exposed; in addition, the scheme introduces a supervisory mechanism in which the trusted center (CA) supervises the anonymous authentication process and can hold the relevant responsible person accountable in case of fraud. Data on the chain can ensure data traceability, but it also brings a certain risk of data leakage, while too much privacy protection can create regulatory difficulties. Li et al.[11] proposed a distributed supervisory privacy protection scheme based on group signature, privacy address protocol, zero-knowledge proof, and attribute encryption. Based on the characteristics of group signature, group administrators can group private key to track and supervise the identity of both sides of group members' transactions.

All the above schemes are implemented based on anonymous authentication techniques and privacy-preserving techniques such as zero-knowledge proofs, which have high security, but also have obvious efficiency problems, i.e., their efficiency decreases with the increase of attributes among test users.

Zhang et al.[12] proposed a supervisable digital currency model using a dual chain structure of coalition chain-public chain, using the coalition chain as the core participant of

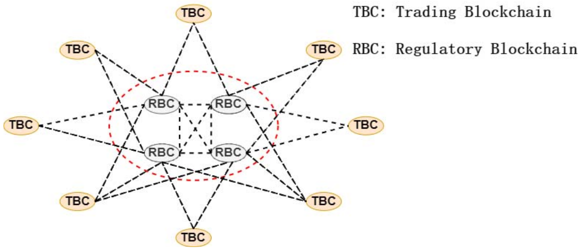

Fig. 3. Dual-chain model.

consensus to ensure the privacy of user transaction data through secret sharing and also designed to achieve controlled anonymity by voting to complete the decryption of transaction contents. Using the public chain as the operational base makes it possible for ordinary users to participate and witness the maintenance of the system. Peng et al.[13] proposed a dual-chain model of content blockchain and regulatory blockchain to solve the supervision problem in the digital content sharing system, combining InterPlanetary File System (IPFS) with blockchain technology to ensure the safe storage and access control of the content, where the supervisory chain even supervises the whole process of the transactions in the system by accepting the request sent by the user and verifying whether the request meets the required specification, and if a supervisory node finds that a user shares bad data or has illegal transactions, it immediately cancels the user's certificate to prohibit further dissemination of bad data.

As shown in Fig.3, the dual-chain model can also regulate illegal transactions by tracing and identity confirmation of blockchain node transactions while maintaining the decentralized feature of blockchain. The regulatory node in the regulatory blockchain can effectively supervise illegal transactions, and the verification node can protect the privacy and security of trading nodes and check the correctness of smart contract results. The regulatory blockchain and trading blockchain run in parallel, which can further improve the efficiency of transactions and the scalability of the system. However, the implementation of the dual-chain model is a very complex algorithm, especially the coupling of the consensus mechanisms of the regulatory and transaction blockchains, which still needs further research.

In addition to the above technology, regulators can also join the consortium blockchain in the form of nodes. Through the full traceability and audit analysis of data, the business in the consortium blockchain can achieve penetrating regulation. At the same time, the regulator can be given some operational authority, such as blacklisting and account freezing. This kind of regulation is unified, transactional, undeniable and irresistible.

C. Public Chain Active Discovery and Exploration Disposition Techniques

Public chain active discovery and exploration refers to how to discover a running public chain in the network world. And the current research mainly focuses on public chains with service functions that have developers or communities running and maintaining them. As of 2021, there are nearly 20,000 types of digital tokens released on the Internet alone, and just looking at the top 200 public chains in the world, we can find that the quality code contributors are mainly concentrated in the top 20, which makes most public chains lack management and maintenance, resulting in most of them being basically zombie chains. The major task of proactive discovery and exploration of public chains is to target public chains that are active in gray areas, circumventing regulation and creating risk hazards through illegal crimes. For a public chain that is being maintained, we can crawl the network information by using the technical set of Internet public opinion, extract features and build classifiers through mining and analysis of public chain data to detect and predict the operation status of the public chain, so as to achieve the role of security risk prevention.

At present, the most research on public chain active discovery and exploration is still by collecting a large amount of historical data and filtering the behavioral characteristics of public chain nodes from it, and detecting, classifying and predicting abnormal behaviors based on mathematical models, etc.

The K-Nearest Neighbor (KNN) algorithm is a theoretically mature machine learning algorithm.Chen et al [14] proposed a KNN-based blockchain anomaly transaction detection scheme by randomizing the transaction data using matrix multiplication of bookkeeping nodes, and then the cloud server detects the anomalous features of the randomized transaction data using the KNN algorithm. The scheme achieves efficient anomaly detection and yet ensures the privacy of the consortium blockchain transactions. However, the disadvantage of KNN algorithm is that it is computationally intensive and needs to calculate the distance of each transaction data to be classified to the whole known samples. Besides, the balance of samples is also one of the problems to be solved. But the matrix randomization approach presented in [14] only blinds transaction features, making it marginally less secure for high-sensitivity application cases.

By abstracting financial fraud as an anomaly detection problem, Liu et al.[15] constructs a heterogeneous graph transformer network suitable for smart contract anomaly detection to classification of node embeddings from neural networks to detect financial fraud on the Ethernet platform. The system uses graph transformation network to learn heterogeneous graph meta-paths, and improves efficiency by avoiding manual given meta-paths. Account features and code features are used as node attributes, but heterogeneous high-order information can be further considered to obtain more effective features. Wu et al.[16] designed two different community detection methods for the bitcoin network and the Ethernet network, and for the bitcoin network, a specific clustering algorithm derived from spectral clustering algorithm is proposed for finding communities in bitcoin network. For the Ethernet network, a bipartite social graph based on smart contract transactions is defined and a new community detection algorithm for low-level signals on the graph can help to find user communities based on user token subscriptions.

By reading the literature, it seems that there are few studies on active discovery for public chains. Most of them analyze the transaction data or smart contracts for existing public chains to discover the behavioral characteristics of existing public chains, such as gambling, fraud and other illegal behaviors. Currently, China, the United States and other countries have recorded the known blockchains. But for the blockchains that are still running on the Internet without record, we need to use the active discovery, detection and disposal technologies of public chains to discover and regulate them. For the above situation, we can study the mining of malicious blockchain application patterns and the automatic detection of malicious blockchain applications.

D. Chain Governance

Chain-based governance can be simply understood as the governance of blockchain and its applications through blockchain technology. The chain-based governance discussed here is mainly on the chain governance. By means of intelligent contracts and consensus mechanisms, the laws and contract terms governing blockchain are transformed into code, and the autonomous governance of blockchain applications is promoted through the operation of blockchain networks.

Compliance means following a rule, such as a norm, policy, standard, or law. This paper understands compliance regulation in the context of chain-based governance to ensure that the corresponding blockchain applications in their risk areas comprehend and take steps to comply with requirements such as relevant laws, policies and regulations in order to achieve their objectives. These requirements can be mandatory national or local regulatory requirements, industry standards, bilateral or multilateral trade agreements, etc. Referring to the compliance regulation process in the supply chain, a good and effective compliance regulation should consider a series of factors such as regulatory requirements, industry standards, organizational norms, and stakeholder interests.

Ethereum has regulated the behavior of smart contracts through Ethereum Request for Comment (ERC), and from ERC20 to ERC1400, ethereum has shifted from avoiding regulation to embracing it. While ERC20 only requires the issuance and transfer of tokens, ERC1400 requires contracts to provide relevant legal documents for issuing security-based tokens and to provide readable explanations of the results of transfer restriction judgments before executing transfers, so that functions such as position locking, Know Your Customer/Anti-money Laundering (KYC/AML) verification, and entry freeze can be implemented at the contract level. In addition to Ethereum's move from avoiding regulation to embracing it, Libra, launched by Facebook, also released a white paper version 2.0 in 2020 to address regulatory concerns. In addition to actions such as due diligence by the association on designated resellers and members, the association has included compliance controls such as Virtual Asset Service Provider (VASP) certification and non-custodial wallet restrictions directly in the Libra protocol, making certain compliance requirements mandatory for all transactions on the Libra blockchain.

Fintech companies generally have weak internal control mechanisms, inadequate consumer protection, opaque information, and increasing crossover and correlation of financial products, making risks difficult to identify and more concealed, making regulation more difficult. The BoYa Regchain provides the RegLang, a smart contract programming language for regulatory technology, and the syntax rules and type system of the contract are designed according to regulatory needs, which facilitates the digitization of regulatory rules and quickly completes the construction of a digital regulatory rule base. Regulators can automatically realize penetrating regulation through smart contracts, and regulatory targets can enhance automated compliance through regulatory rules published by regulators. Lu et al.[17] designed the OriginChain system to provide transparent tamper-proof traceability data, enhances the data's availability, and automates regulatory-compliance checking. The system can generate smart contracts representing legal agreements by codifying a combination of services and other conditions defined in the agreement so that the smart contracts can automatically check and enforce these conditions. It also checks whether all the information required by the regulation is provided to enable automated regulatory compliance checks.

The governance mechanism of chain governance is not yet perfect, and regulators can code the rules to achieve partial internal governance of the blockchain by developing new specifications in different forms. Smart contracts are the best way to achieve compliance regulation, which can automate the system and reduce regulatory costs through smart contracts. However, both smart contracts and blockchain compliance regulation are just getting started, and there are still more problems to be solved, such as smart contract loopholes and other issues. At the same time, the research and development of a set of perfect blockchain technical standards and specifications is also a prerequisite to guaranteeing the safety and reliability of blockchain system construction and application.

Here, we summarize the technologies mentioned in the above four research directions and show the characteristics of each technology in Table 1.

In Table 1, we can see that coalition chains are less difficult to regulate than public chains, and the technologies that can be adopted are more diversified. Besides, it can also be concluded that the main idea of blockchain regulation at present is still blockchain traceability and characterization based on transaction data. However, compliance regulation, although less studied at present, has more growth space and is well worth studying.

IV. Conclusion

In this paper, we can notice that the technical approach based on statistical methods and compliance regulation are major research ideas in regulatory technology currently. However, the former must identify and train aberrant behaviors among them using already available transaction data, and the

TABLE I
CHARACTERISTICS OF EACH REGULATORY TECHNOLOGY MENTIONED IN THE FOUR RESEARCH DIRECTION

References	Privacy Protection	Adaptability	Regulatory efficiency	Type of Regulation
Shen et al.[7]	×	Public chain	High	Feature Analysis
Zheng et al.[8]	×	Public chain	High	\
Steven et al.[9]	×	Public chain	High	Feature Analysis
Wang et al.[10]	√	Consortium Blockchain	Low	Traceability
Li et al.[11]	√	Consortium Blockchain	Low	Traceability
Zhang et al.[12]	√	Consortium/Public chain	High	Traceability
Peng et al.[13]	√	Consortium/Public chain	High	Traceability
Chen et al.[14]	√	Consortium Blockchain	High	Feature Analysis
Liu et al.[15]	√	Public chain	High	Feature Analysis
Wu et al.[16]	×	Public chain	High	Feature Analysis
Lu et al.[17]	√	Consortium/Public chain	High	Compliance Check

process from creation to accurate prediction of new anomalous behavior may result in significant losses. While the latter faces the problem of how to correctly interpret the compliance requirements through the code as well as rule updates, which is still in the initial stage. More importantly, blockchain application scenarios are complex and have diverse needs. In response to the above problems, we list several future directions:

- Blockchain compliance regulation, where changes are made at the code layer and technology layer based on the relevant characteristics of smart contracts and blockchain to promote blockchain intelligence and regulatory code compliance through underlying compliance and technology compliance.
- Blockchain traceability system gathers and analyzes transactions using deep learning and statistical approaches to identify aberrant behavior in blockchain applications and continually optimizes the regulatory model as transactions progress.
- A compliance regulation model is designed to integrate regulation into the operation of the blockchain to realize the regulation and traceability of data information within the system while protecting user privacy. In addition, we can investigate the compliance standards of various industries and extract common compliance rules to make the compliance regulation model more adaptable.

ACKNOWLEDGMENT

I would like to thank my thesis committee members for all of their guidance through this process; your discussion, ideas, and feedback have been absolutely invaluable.

REFERENCES

[1] X. Yang, K. Wei, S. D. Qing, Q. Zhang, B. X. Yang, and Y. K. Zhang, “Blockchain security whitepaper,” Trustworthy Blockchain Advancement Program, pp. 20–25, 2018.

[2] C. Chen, “Key technologies of federated blockchain and regulatory challenges of blockchain,” Power Equipment Management, no. 11, pp. 20-21+28, 2019.

[3] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, “Community politics and regulation,” in Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, pp. 168–189, 2016.

[4] O. Marian, “Are Cryptocurrencies Super Tax Havens,” Mich. L. Rev. First Impressions, vol. 112, 2013, pp. 38–48.

[5] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, and G.M.Voelker, “A fistful of bitcoins: characterizing payments among men with no names,” in Proceedings of the 2013 conference on Internet measurement conference, Barcelona Spain, pp. 127–140, Oct. 2013.

[6] P. De Filippi, “Characteristics of blockchains,” in Blockchain and the Law, Harvard University Press, pp. 33–60, 2018.

[7] M. Shen, A. Sang, L. Zhu, R. Sun, and C. Zhang, “Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency,” Chin J Comput, vol. 1, pp. 193–208, 2021.

[8] L. Zheng, X. Helu, M. Li, and H. Lu, “Automatic discovery mechanism of blockchain nodes based on the Kademlia algorithm,” in International Conference on Artificial Intelligence and Security, pp. 605–616, 2019.

[9] S. Farrugia, J. Ellul, and G. Azzopardi, “Detection of illicit accounts over the Ethereum blockchain,” Expert Systems with Applications, vol. 150, p. 113318, 2020.

[10] Z. Wang, J. Fan, L. Cheng, H. Z. An, H. B. Zheng, and J. X. Niu, “Supervised anonymous authentication scheme,” Journal of Software, vol. 30, no. 6, pp. 1705–1720, 2019.

[11] L. Li, H. N. Du, and T. Li, “Blockchain supervisable privacy protection scheme based on group signature and attribute encryption,” Computer Engineering, vol. 48, no. 06. pp. 132–138, 2022.

[12] J. Y. Zhang, Z. Q. Wang, Z. L. Xu, Y. F. Ouyang, and T. Yang, “A regulatable digital currency model based on blockchain,” Computer Research and Development, vol. 55, no. 10, pp. 2219–2232, 2018.

[13] R. Y. Peng, Z. F. Ma, and S. S. Luo, “Research and implementation of digital content service and security supervision technology based on blockchain,” Netinfo Security, vol. 20, no. 10, pp. 49–56, 2020.

[14] B. J. Chen, F. S. Wei, and C. X. Gu, “Blockchain abnormal transaction detection with privacy-preserving based on KNN,” Netinfo Security, vol. 22, no. 03, pp. 78–84, 2022.

[15] L. Liu, W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng, and M. Liu, “Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum,” Future Generation Computer Systems, vol. 128, pp. 158–166, 2022.

[16] S. X. Wu, Z. Wu, S. Chen, G. Li, and S. Zhang, “Community detection in blockchain social networks,” Journal of Communications and Information Networks, vol. 6, no. 1, pp. 59–71, 2021.

[17] Q. Lu and X. Xu, “Adaptable blockchain-based systems: a case study for product traceability,” Ieee Software, vol. 34, no. 6, pp. 21–27, 2017.