Blockchain Anomaly Transaction Detection: An Overview, Challenges, and Open Issues

Zhiwei Liu[1,3], Haoyu Gao[1,3], Hong Lei[1,2](✉), Zixuan Liu[1,3], and Chao Liu[4]

[1] Hainan University, Haikou 570228, China
liuzhiwei@hainanu.edu.cn, {haoyu,zixuan}@ssc-hn.com,
leiluono1@163.com
[2] SSC Holding Company Ltd, Chengmai 571924, China
[3] Oxford-Hainan Blockchain Research Institute, Chengmai 571924, China
[4] The Blockhouse Technology Limited, Oxford OX2 6XJ, UK
liuchao@tbtl.com

Abstract. In recent years, the rapid development of blockchain technology has attracted a great deal of attention from academia and industry, as it can be applied to a variety of traditional financial and non-financial domains. Blockchain provides decentralized, tamper-evident, and traceable characteristics that enhance the security of these domains. Recent researches have revealed, however, that there are some security abnormalities in the blockchain transaction process, and in order to solve these issues, the detection of the behavior of anomaly transaction is required. In this paper, we initially explore typical and abnormal transactions in blockchain technology before delving deeply into the integration of anomaly transaction detection algorithms in blockchain applications. Then, we examine conventional approaches for anomaly identification and blockchain-based techniques for transactional anomaly detection. Then, a thorough analysis of blockchain anomaly detection models in the financial domain and its application in non-financial domains was presented. Finally, based on the results of the survey, we conclude with future research directions and challenges.

Keywords: Blockchain · Transaction behavior · Anomaly detection · Detection model

1 Introduction

Blockchain, a booming and revolutionary technology, is decentralized, secure, anonymous, traceable, and tamper evident. The successful application of blockchain to digital currencies such as Bitcoin and Ethereum has led to its widespread development in the fintech sector. Blockchain technology is becoming one of the most promising technologies in the next-generation Internet interaction system [1]. In addition to cryptocurrencies, blockchain is proposed as one of the emerging digital industries in the Outline of the 14th Five-Year Plan and 2035 Visionary Goals for National Economic and Social Development of the People's Republic of China, which proposes "to develop blockchain service

X. Qiu et al. (Eds.): ISCC 2023, SIST 350, pp. 126–140, 2024.
https://doi.org/10.1007/978-981-99-7161-9_10

platforms and financial technology, supply chain finance, and government services with a focus on alliance chains." As a result, blockchain technology has been applied to social services, risk management, medical care, and other fields [2]. However, most of the current research focuses on exploring the applications of blockchain technology in these fields, and although the characteristics of blockchain can solve the security and privacy problems that exist in these applications, abnormal behaviors may occur in the blockchain during transactions, reducing the security, privacy, and reliability of these applications. Although there are some studies on the security and privacy issues of blockchain, there is still a lack of systematic investigation into the security issues during the transactions of blockchain systems [3].

Based on the existing studies, blockchain-related application scenarios can be broadly classified into two categories, which are financial domain-related applications [4, 5, 6] and non-financial domain-related applications [7, 8, 9]. Since blockchain technology has natural financial attributes since its inception, it has more extensive and mature applications in the fintech field, and some relevant studies exist on the issue of security [10, 11, 12]. In the applications related to the blockchain financial field, users are making a large number of transactions every day, which are packaged by miners into blocks on the chain, however, there are inevitably some abnormal behaviors in the transaction process, and these behaviors, if not curbed, will disrupt the normal transaction order and harm the personal interests of users. In order to avoid these abnormal transaction behaviors, these studies detect the abnormal transaction behaviors existing in blockchain networks. However, in non-financial fields, such as social governance and government and livelihood scenarios, blockchain-related applications are mostly still in the exploration stage, and relatively few studies have been conducted for the detection of abnormal behaviors in these applications. Therefore, this paper discusses the anomalous behavior of blockchain-related application scenarios in financial and non-financial domains.

The rest of the paper is structured as follows. In Sect. 2, the concept of blockchain transactions is outlined, and blockchain normal and abnormal transactions are discussed separately. Section 3 discusses the anomaly detection methods in the traditional cybersecurity domain, and the characteristics and detection methods of blockchain anomalous transaction behavior. Next, Sect. 4 discusses the use of anomaly detection methods in different scenarios of blockchain, and Sect. 5 discusses future research approaches and challenges. Finally, in Sect. 6 we conclude on the basis of the survey.

2 Blockchain Transaction Behavior Overview

Transactions are a core concept in blockchain systems, and in this section, we discuss the concepts of blockchain normal and abnormal transactions, respectively.

2.1 Blockchain Transaction Definition

Transaction is a very important concept in the blockchain system. We usually regard the blockchain as a distributed ledger that is constantly synchronized in real time, in which any action can be considered as a transaction. After the introduction of smart contracts in blockchain, the contract call can also be regarded as a transaction, so the transaction in blockchain has gone beyond the definition of “value exchange”, and a more precise definition is that the transaction is a record of a transaction in the blockchain. And no matter how big or small the transaction is, it needs the participation of transaction.

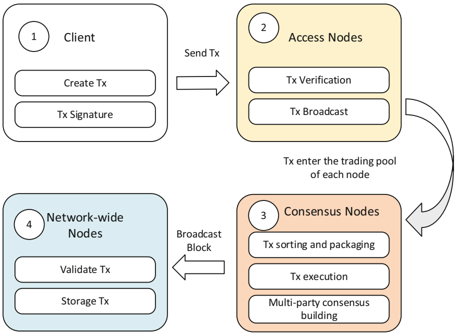

Fig. 1. Blockchain transaction process.

Figure 1 shows how a transaction is added to the blockchain as shown in the transaction flow in the blockchain. The user’s request is given to the client, and the client creates a transaction and digitally signs the transaction; after sending the transaction to the access node, the node verifies the signature of the transaction to determine whether the transaction is legitimate, and the legitimate transaction will be broadcast to other nodes known to the node; next, the transaction is packaged as a block to be consensus, and then sent to each node, and after the node receives the block, it calls the block verifier After receiving the block, the node will call the block verifier to take out the transaction from the block one by one and execute it. Then the blockchain requires the nodes to reach consensus on the execution result of the block before the block can be released, and the node will start to release the block after reaching final consistency through different consensus algorithms; after the block is released by consensus, the node will verify the transaction and store the transaction and execution result in the block to the hard disk permanently.

2.2 Blockchain Abnormal Transaction Definition

In this paper, the complete process of a normal transaction in blockchain is discussed in Sect. 2.1, however, in the actual transaction process, there may be some anomalies, and we call the anomalies that exist in the blockchain transaction process as blockchain anomalous transactions, and in this section, we will introduce the definition of anomalous behavior and the classification of anomalous transactions in blockchain. Anomalous behavior exists widely in various fields, and there are different definitions for anomalies in different application fields. The book [13] classifies exceptions into three categories in the following manner, namely, point exceptions, contextual exceptions, and set exceptions.

Different from the above abnormal classification methods, blockchain abnormal transactions can be divided into two categories, one is the abnormal behavior generated by blockchain transactions themselves due to technical risks, and the other is the abnormal behavior that exists through analysis based on the data generated by blockchain transactions. The first category is the vulnerability arising from the risk of technical vulnerability or imperfect design of consensus algorithm in the process of blockchain transactions. Typical abnormal transaction behaviors exist due to technical risk, such as double flower attack, routing attack, 51% attack, etc. The second category is to analyze the data generated in blockchain transactions to conclude the existence of abnormal transactions, and such typical abnormal transaction risks include money laundering transactions, Ponzi schemes, fraudulent transactions, extortion transactions, etc.

3 Blockchain Abnormal Transaction Detection Analysis

This section first introduces the analysis framework of traditional anomalous behavior detection techniques, and then introduces the characteristics of blockchain anomalous transaction behavior and the corresponding detection methods.

3.1 Traditional Anomaly Detection Methods

In the traditional field of cybersecurity, anomaly detection is a very important data analysis task, which detects anomalous behavior from a given data set, and the increasing complexity of the network environment of the Internet has prompted the continuous updating of detection tools. Anomaly detection has been extensively studied in statistics and machine learning [14], while it is also known as outlier detection, novelty detection, deviation detection, and anomaly mining. Researchers have different definitions of anomalies in different fields, and Hawkins [15] gives a more universal definition: "An anomaly is an observation that deviates so much from other observations that it raises suspicion that it was generated by a different mechanism". In addition to the field of cyber security, anomaly detection techniques are also widely used in healthcare, public health, fraud detection, intrusion detection, image processing, and other fields [16].

Figure 2 shows the traditional framework for network anomaly detection, where the input data is processed and then anomaly detection is performed in two ways (supervised, unsupervised), and the output results obtained are evaluated using a score-following-label situation [17]. The advantage of this generic framework for network anomaly detection is its simplicity, and the disadvantage is that the input data needs to be processed and only a single anomaly detection can be performed for different data types. This detection framework is also applicable in the field of blockchain anomaly transaction behavior detection due to the more uniform blockchain transaction data types. There are still some research challenges in the area of traditional network anomaly detection [17], despite the many available detection techniques, and current intrusion detection techniques are time-sensitive [18]. Anomaly detection techniques need to be continuously updated.

This section introduces that anomaly detection is widely used in various fields and there are some challenges in the traditional network security anomaly detection field, which also exist in blockchain anomalous transaction behavior detection. The next section focuses on how to extract and detect anomalous transaction behavior features of blockchain.

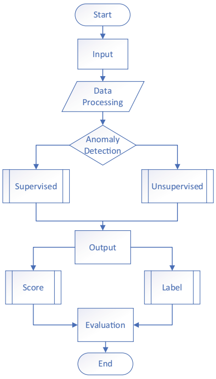

Fig. 2. General framework for traditional network anomaly detection

3.2 Blockchain Abnormal Transaction Behavior Feature Extraction and Detection

The literature [19] summarizes and analyzes the abnormal transaction behavior in blockchain from the basic features of smart contracts and the topology of blockchain networks, and the paper mentions that the behavioral features of Ponzi scheme, game gambling contract and social network contract in smart contracts can be constructed by the 14 basic features proposed by Hu et al. [20] to improve the recognition rate of smart contract classification. The study is to identify abnormal transactions by analyzing the features of the transactions to make judgments on the transaction patterns.

How to extract the features of abnormal trading behavior, different methods are used in [21], and to study whether there is market manipulation due to the drastic price fluctuations of cryptographic digital currencies, it uses complex networks to model users and transactions, proposes a framework for dynamic trading network analysis, uses Singular Value Decomposition (SVD) method to analyze the trading fluctuations of the network and found a great correlation between abnormal user behavior and price fluctuations, as shown in Abnormal transaction behavior Table 1, for six abnormal trading behaviors of users. These abnormal trading behaviors, except for the self-loop, each transaction between users is a normal transaction, but because there are too many transactions in a short period of time, the set of these transactions is judged as abnormal, which is also mentioned in the literature [13] for the set of abnormalities. However, the pattern of abnormal trading behavior obtained in this way to determine the abnormal behavior has some problems, and if a large number of accounts are created for trading at the same time, they can avoid being detected by this method, because there are a large number of accounts in the hands of some institutions.

To solve the problem of multiple account transactions, the attribution of accounts needs to be clarified, and the complex holding, and trading relationships in the market should be clarified, and the accounts in the virtual space should be related to the entities in reality. The complex relationships between entities and various accounts in the token ecosystem are revealed in the literature [22] by describing the characteristics of token creators, holders, and trading transfer activities, and by constructing an Ethereum token

Table 1. Abnormal transaction behavior

Abnormal transaction behavior	Description	Anomaly factors	Detected anomaly
Self-circulation	An account made 749 trades with itself	Self-Tx Tx frequency	Illegal Tx
Unidirectional	Account A made 322 sell trades to account B	Tx frequency	Malicious Tx
Bidirectional	Account A and account B traded with each other more than 150 times	Tx frequency	Malicious users
Triangular	There is a triangle-like structure between the three accounts	Recurring Tx	Malicious Tx
Polygonal	Many accounts form a polygon-like group	Recurring Tx	Malicious Tx group
Star-shaped	The star model has a core account that buys or sells bitcoins to many accounts	Tx Number	Malicious accounts

transaction network framework, using graph analysis, and proposing an algorithm to discover the potential relationships between tokens and other accounts. The literature [21] answers the association relationship between entities and accounts but does not explain why these entities hold these accounts.

When an account is determined to be an abnormal account, it is clear that transactions between abnormal accounts are abnormal transactions, and therefore the identification of abnormal accounts has been the focus of research in recent years. Previously machine learning methods [12, 23] were used to automatically detect anomalous contract accounts, however it was difficult to accurately identify the characteristics of anomalous contracts and obviously statistical analysis based on that contract was also invalid, and secondly overfitting of the model was caused by ignoring the imbalance and repetitiveness of smart contract accounts. In Ref. [24], the authors propose a data-driven robust method for detecting abnormal contract accounts in Ethereum, which first collects both abnormal and normal contract data from Ethereum to solve the problem of data imbalance. Next three types of feature sets are defined and combined to obtain a more comprehensive set of features.

4 Blockchain Anomaly Transaction Detection

In this section, we have discussed the blockchain anomaly transaction checking model in the financial domain and the blockchain application in the non-financial domain, respectively.

4.1 Financial Field

Blockchain technology has natural advantages in the field of fintech, so it has also been very widely used in the field of finance [4, 5, 6], bringing a brand new change to the development of the financial industry. However, the rapid development has also generated many related security and business risks, such as money laundering transactions, financial fraud, Ponzi schemes, market manipulation and other problems, which have brought heavy obstacles to the development of blockchain in the field of fintech. This section provides an in-depth study on the financial application scenarios of money laundering transactions and abnormal transactions detection in Ponzi schemes. The research related to transaction detection is analyzed in depth, as shown in Table 2.

Money Laundering Transactions. Due to the decentralized, and anonymous nature of blockchain, etc., It facilitates the transfer of funds for unscrupulous individuals. With the emergence of bitcoin and ethereum, it has further facilitated money laundering transactions and other illegal and criminal acts. In all major digital currency exchanges, there are unusual transactions for money laundering, and how to discern which transactions are money laundering transactions is gradually becoming a focus of blockchain researchers.

Teichmann et al. [25] showed that cryptocurrencies are a very suitable tool for money laundering, terrorism financing and corruption and that current compliance efforts in the field of cryptocurrencies are ineffective. The literature [26] specifically analyzes the risks associated with the uncontrolled use of blockchain technology by civil society, financial organizations, regulators, and law enforcement agencies, with a particular focus on the risks of money laundering through blockchain technology. Guerra et al. [27] analyze the problem of money laundering through crypto-assets and propose an approach to transnational anti-money laundering operations that uses tracking and reverse engineering anonymity techniques to track cryptocurrency transaction history, as well as employing a global blacklist of crypto-asset prefixes to prevent money laundering. Maksutov et al. [28] investigated transaction anonymization methods using a decentralized approach based on Coin Join transactions and showed that tracking Coin Join transactions is feasible to determine the fact that users are involved in creating transactions, providing additional advantages. Alarab et al. [29] performed a comparative analysis of the performance of classical supervised learning methods by using a recently published dataset from the Bitcoin blockchain to predict legal and illegal transactions in the network. Oad et al. [30] proposed a Blockchain-enabled Transaction Scanning (BTS) method to detect anomalous behavior, the BTS method specifies rules for outlier detection and fast flow of funds to limit anomalous behavior in transactions, and according to experimental results, the proposed BTS method automates the process of investigating transactions and limits the incidents of money laundering. Karasek-Wojciechowicz et al. [31] proposed Distributed Ledger Technology (DLT) based permissionless network, while ensuring the protection of personal data according to the EU General Data Protection Regulation (GDPR) rules, addressing the risk of money laundering and terrorist financing arising from anonymous blockchain spaces or exchanges with strong pseudonyms. Because virtual asset service providers are unable to identify originators and beneficiaries, Park et al. [32] propose a distributed ledger technology (DLT) based customer identification service model that enables virtual asset service providers to verify the identity of originators and beneficiaries. Other influential work includes [33], which explores the extent to which permissionless blockchain transactions can disrupt the current anti-money laundering (AML) regime and enforcement efforts, respectively.

Ponzi Scheme. In the financial field, blockchain is more likely to be packaged by unscrupulous elements as a ponzi scheme for fraud due to its complex technical principles and various financial projects. a ponzi scheme is a typical financial investment fraud scam that gives old investors lucrative interest and returns by continuously absorbing new investors' funds to create the illusion of making money to pull in more investments until the capital chain breaks and collapses, the organizers are unable to repay the principal and interest, and investors are left with nothing; Ponzi schemes have been found to scam considerable assets on the blockchain, which brings a very negative impact on blockchain technology.

To help deal with these problems, Chen et al. [23] proposed an approach to detect Ponzi schemes on the blockchain by using data mining and machine learning methods. Jung et al. [34] proposed an improved approach to provide a detection model for Ponzi schemes on Ethereum using data mining to benchmark several classification algorithms using Weka to obtain a model that simultaneously achieving high accuracy and high recall. Chen et al. [12] collected real-world samples to propose a classification model to detect smart Ponzi schemes, and by using the proposed approach, it is estimated that there are more than 500 smart Ponzi schemes running on Ethereum. Lou et al. [35] proposed an improved convolutional neural network as a detection model for Ponzi schemes in smart contracts. Bian et al. [36] proposed an image-based scam detection method using an attention capsule network focused on Ethereum. Chen et al. [37] proposed a semantic-aware Ponzi scam detection method for identifying Ponzi scams in Ethereum smart contracts. Fan et al. [38] introduced a new method to detect smart Ponzi schemes in blockchain, proposing an Anti-leakage Smart Ponzi Schemes Detection (Al-SPSD) model based on the idea of ordered boosting. Yu et al. [39] proposed a graph convolutional network (GCN)-based detection model to accurately distinguish Ponzi schemes contracts on different real-world Experiments on the Ethereum dataset show that the proposed model is effective in detecting Ponzi schemes compared to general machine learning methods.

Jin et al. [40] proposed a generic Heterogeneous Feature Augmentation module (HFAug) that can be combined with existing Ponzi scheme detection methods, and the experimental results showed the effectiveness of heterogeneous information for detecting Ponzi schemes. In their latest study, Jin et al. [41] introduced the Time-aware Metapath Feature Augmentation (TMFAug) module as a plug-and-play module that can help existing Ponzi scheme detection methods achieve significant performance improvements on Ethereum net datasets. TMFAug module, as a plug-and-play module, TMFAug can help existing Ponzi scheme detection methods achieve significant performance improvements on the Ethereum dataset, demonstrating the effectiveness of heterogeneous temporal information for Ponzi scheme detection.

4.2 Non-Financial Field

With the in-depth research on blockchain technology, its development in non-financial fields has also been rapid. Most of the current research is aimed at the exploration of blockchain technology in these application scenarios, with less attention to security

Table 2. Blockchain anomaly transaction detection in financial application scenarios.

Ref no	Main objective	Detected anomaly	Methods/Algorithm	Dataset
[27]	Proposes a framework of anti-money laundering principles with a focus on cryptocurrencies	Money laundering consolidation	Global crypto asset prefix blacklist	N/S
[28]	Detecting transactions involved in money laundering schemes	Money laundering transactions	Track coin join transactions	N/S
[29]	Compare classical supervised learning methods	Illegal Transactions	Aggregate Learning	Bitcoin Dataset
[30]	Blockchain-enabled Transaction Scanning	Money laundering transactions	Transaction scanning	N/S
[31]	License-free networks based on distributed ledger technology	Money laundering transactions	Unlicensed networks	N/S
[23]	Detecting Ponzi schemes on the blockchain through machine learning	Ponzi scheme	Machine learning	N/S
[34]	Using data mining to provide a detection model for Ponzi schemes on Ethereum	Ponzi scheme	Data mining	Ethereum
[12]	Detecting Ponzi Schemes Implemented as Smart Contracts on Blockchain	Ponzi scheme	Extraction of two types of features from the transaction history and operation code of smart contracts	Ethereum
[35]	An Intelligent Ponzi Scheme Detection Model Based on Improved Convolutional Neural Network	Ponzi scheme	Improved convolutional neural network	Ethereum

(*continued*)

issues. This section introduces the traceability and deposition applications of blockchain

Table 2. (*continued*)

Ref no	Main objective	Detected anomaly	Methods/Algorithm	Dataset
[36]	An image-based scam detection method	Ponzi scheme	Attention Capsule Network (SE-CapsNet)	Ethereum
[37]	A Semantic-Aware Ponzi Scheme Detection Method	Ponzi scheme	Semantic perception	Ethereum
[38]	An anti-leakage intelligent Ponzi scheme detection model based on the idea of ordered lifting is proposed	Ponzi scheme	Target statistics	Ethereum
[39]	A graph convolutional network (GCN) based detection model is proposed to accurately distinguish Ponzi scheme contracts	Ponzi scheme	GCN	Ethereum
[40]	Propose a generic heterogeneous feature enhancement module	Ponzi scheme	Capturing heterogeneous information related to account behavior patterns	Ethereum

technology in the non-financial field and discusses the challenges and future research directions in this field in the next chapter.

Supply Chain Traceability. With the rapid development of internet technology, a large number of emerging technologies have been applied to supply chain traceability systems; however, these current systems are centralized, opaque and monopolistic, which can lead to trust problems [42]. Blockchain technology has been applied to the field of supply chain traceability as a novel approach due to its decentralized and information traceability characteristics. However, the current blockchain-related research for supply chain traceability focuses on the exploration of applications and ignores the security risks in the blockchain transaction process, which brings certain obstacles to the development of blockchain technology.

Gálvez et al. [43] investigated the potential of blockchain technology to guarantee traceability and authenticity in the food supply chain. Caro et al. [44] proposed AgriBlockIoT, a fully decentralized, blockchain-based traceability solution for agri-food supply chain management that seamlessly integrates IoT devices that produce and consume digital data. Westerkamp et al. [45] proposed a blockchain-based supply chain traceability system using smart contracts. Salah et al. [46] proposed a method to efficiently execute business transactions using Ethereum blockchain and smart contracts for soybean tracking and tracing throughout the agricultural supply chain. The current prefabricated component supply chain management often faces challenges such as fragmentation, poor traceability, and lack of real-time information. To address these challenges, Wang et al. [47] developed a novel blockchain-based information management framework for precast supply chains that extends the application of blockchain in the construction supply chain domain. The contribution of Behnke et al. [48] is to identify boundary conditions for sharing guaranteed information to improve traceability. Shahid et al. [49] developed a novel blockchain-based information management framework for agricultural and food (Agri-Food) supply chain proposed a complete solution, the proposed traceability system writes all transactions to the blockchain and uploads the data to the Interplanetary File System (IPFS) to ensure the efficiency, security and reliability of the system.

Electronic Evidence. Blockchain technology solves some problems that arise in the collection, identification, storage and application of traditional electronic evidence, such as the possibility of tampering with evidence by forensic personnel cannot be ruled out, and the credibility of forensic tools is not verified and it is difficult to obtain evidence in a timely manner; using blockchain technology for forensics can reduce manual participation and exclude falsification by forensic personnel, and the credibility of forensic tools will be verified first during forensics. it can collect evidence quickly and prevent evidence from being replaced.

To ensure the authenticity, invariance, and auditability of electronic evidence, existing studies have used blockchain and related extensions. Tsai et al. [50] proposed a regulatory blockchain framework to facilitate the security and transparency of digital evidence during criminal investigations, which is implemented on an Ethereum smart contract to support the authenticity and digital evidence in the preliminary investigation, case management, and courtroom phases. Tian et al. [51] proposed a secure digital evidence framework using blockchain, which has a loosely coupled structure in which evidence and evidentiary information are maintained separately and only evidentiary information is stored in the blockchain while evidence is stored in a trusted storage platform. Kim et al. [52] proposed a two-level blockchain system that separates digital evidence into a hot blockchain and a cold blockchain in the process of criminal investigation, frequently changing information is stored in the hot blockchain, while unchanging data such as videos are stored in the cold blockchain. Miao et al. [53] address the data authenticity and integrity problems of traditional electronic evidence storage methods and the failure of existing blockchain storage schemes to consider storage cost and efficiency well; proposed an electronic evidence storage model that uses directed acyclic graph to optimize the on-chain storage efficiency of electronic evidence.

5 Challenges and Future Research Directions

5.1 Blockchain in Finance for Abnormal Transaction Detection

Key Challenge. According to our analysis of anomalous transaction detection models for blockchain-based applications related to the financial sector, we did not find any discussion on privacy protection in the related work. Stakeholders in blockchain networks are reluctant to share their complete data because complete privacy guarantees are not available.

Future Research Directions. The problem of protecting user privacy in anomalous transaction detection in blockchain needs to be addressed, and how to balance the relationship between privacy issues and anomaly detection issues is an urgent problem for relevant researchers to solve. To solve these problems, researchers can adopt methods such as differential privacy and zero-knowledge proof.

5.2 Blockchain in the Non-Financial Sector for Anomalous Transaction Detection

Key Challenges. The research on blockchain in the non-financial field mainly focuses on application-related exploration, and not enough attention is paid to the security issues in it. As the application of blockchain in the non-financial field gradually increases, the next research needs to increase the research on the security of blockchain in this field, especially the research on the abnormal transaction behavior in the non-financial application of blockchain is often easily ignored by the researchers.

Future Research Direction. Research is needed on the detection of abnormal behavior of blockchain transactions in the non-financial field, and how to solve the regulatory problems in blockchain transactions is an important problem that researchers need to solve.

6 Conclusion

With the emergence and popularity of digital cryptocurrencies, applications related to blockchain technology have attracted great interest from academia and industry. The decentralized nature of blockchain makes it a secure and trustworthy application platform, and it is widely used in various fields. Although blockchain is more secure and reliable compared to ordinary computer networks, it still has some vulnerabilities and is susceptible to malicious attacks. In order to ensure the safe operation of blockchain application platforms, abnormal transaction behaviors need to be identified in a timely manner. Therefore, anomaly detection techniques have started to be studied to identify abnormal behaviors in blockchain networks. In this paper, we dive into a comprehensive survey of anomalous transaction detection models in blockchain. First, we present the development of theoretical approaches related to anomaly detection in the traditional network security domain. Then, we discuss the researches related to the area of blockchain anomalous behavior detection and provide a detailed survey of anomalous transaction detection in the financial domain and related application research in the non-financial domain. Finally, we provide a comprehensive discussion of the challenges and future research directions that researchers in the area of anomalous transaction detection in blockchain systems need to focus on.

Acknowledgements. 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 (No. 62163011); in part by the Research Startup Fund of Hainan University under Grant KYQD(ZR)-21071.

References

1. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: A survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)
2. Monrat, A.A., Schelén, O.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
3. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Futur. Gener. Comput. Syst. **107**, 841–853 (2020)
4. Karagiannis, I., Mavrogiannis, K., Soldatos, J., Drakoulis, D., Troiano, E., Polyviou, A.: Blockchain based sharing of security information for critical infrastructures of the finance sector. In: International Workshop on Information and Operational Technology Security Systems. International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity, International Workshop on Security for Financial Critical Infrastructures and Services pp, pp. 226–241. Springer, Cham (2020)
5. Huckle, S., Bhattacharya, R., White, M., Beloff, N.: Internet of things, blockchain and shared economy applications. Proc. Comput. Sci. **98**, 461–466 (2016)
6. Moncada, R., Ferro, E., Favenza, A., & Freni, P.: Next Generation Blockchain-Based Financial Services. In: European Conference on Parallel Processing pp. 30–41. Springer, Cham (2021)
7. Wang, Z., Wang, L., Chen, Q., Lu, L., Hong, J.: A traditional chinese medicine traceability system based on lightweight blockchain. J. Med. Internet Res. **23**(6), e25946 (2021)
8. Kumar, R., & Tripathi, R.: Traceability of counterfeit medicine supply chain through Blockchain. In: 2019 11th international conference on communication systems & networks (COMSNETS) pp. 568–570. IEEE, (2019)
9. Wang, L., Ma, Y., Zhu, L., Wang, X., Cong, H., Shi, T.: Design of integrated energy market cloud service platform based on blockchain smart contract. Int. J. Electr. Power Energy Syst. **135**, 107515 (2022)
10. Badawi, E., Jourdan, G.V.: Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. IEEE Access **8**, 200021–200037 (2021)
11. Chatzigiannis, P., & Chalkias, K.: Proof of assets in the diem blockchain. In International Conference on Applied Cryptography and Network Security pp. 27–41. Springer, Cham (2021)
12. Chen, W., Zheng, Z., Ngai, E.C.H., Zheng, P., Zhou, Y.: Exploiting blockchain data to detect smart ponzi schemes on ethereum. IEEE Access **7**, 37575–37586 (2019)
13. Ben-Gal, I.: Outlier detection. In Data mining and knowledge discovery handbook pp. 131–146. Springer, Boston, MA (2005)
14. Pathan, A. S. K. (Ed.).: The state of the art in intrusion prevention and detection (Vol. 44). Boca Raton, CRC press (2014)
15. Hawkins, D.: Identification of Outliers (Monographs on Statistics and Applied Probability) (2013)
16. Ahmed, M., Anwar, A., Mahmood, A. N., Shah, Z., & Maher, M. J.: An investigation of performance analysis of anomaly detection techniques for big data in Scada systems. EAI Endorsed Trans. Ind. Networks Intell. Syst., 2(3), e5 (2015)

17. Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**, 19–31 (2016)
18. Chao, H.C.: Dependable multimedia communications: Systems, services, and applications. J. Netw. Comput. Appl. **34**(5), 1447–1448 (2011)
19. Han, H., Chen, Y., Guo, C., & Zhang, Y.: Blockchain Abnormal Transaction Behavior Analysis: a Survey. In International Conference on Blockchain and Trustworthy Systems pp. 57–69. Springer, Singapore (2021)
20. Hu, T., Liu, X., Chen, T., Zhang, X., Huang, X., Niu, W., ... & Liu, Y.: Transaction-based classification and detection approach for Ethereum smart contract. Inform. Process. Manag. 58(2), 102462 (2021)
21. Chen, W., Wu, J., Zheng, Z., Chen, C., & Zhou, Y.: Market manipulation of bitcoin: Evidence from mining the Mt. Gox transaction network. In: IEEE INFOCOM 2019-IEEE conference on computer communications pp. 964–972. IEEE, (2019)
22. Chen, W., Zhang, T., Chen, Z., Zheng, Z., Lu, Y.: Traveling the token world: A graph analysis of ethereum erc20 token ecosystem. In Proceedings of The Web Conference **2020**, 1411–1421 (2020)
23. Chen, W., Zheng, Z., Cui, J., Ngai, E., Zheng, P., & Zhou, Y.: Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In: Proceedings of the 2018 world wide web conference, pp. 1409–1418 (2018)
24. Aljofey, A., Rasool, A., Jiang, Q., Qu, Q.: A feature-based robust method for abnormal contracts detection in ethereum blockchain. Electronics **11**(18), 2937 (2022)
25. Teichmann, F. M. J., & Falker, M. C.: Cryptocurrencies and financial crime: solutions from Liechtenstein. J. Money Launder. Control (2020)
26. Amosova, N., Kosobutskaya, A. Y., & Rudakova, O.: Risks of unregulated use of blockchain technology in the financial markets. In 4th International Conference on Economics, Management, Law and Education (EMLE 2018) pp. 9–13. Atlantis Press (2018)
27. Guerra, G.R., Marcos, H.J.B.: Legal remarks on the overarching complexities of crypto anti-money laundering regulation. Revista Juridica **4**(57), 83–115 (2019)
28. Maksutov, A. A., Alexeev, M. S.: Detection of blockchain transactions used in blockchain mixer of coin join type. In: 2019 IEEE conference of russian young researchers in electrical and electronic engineering (EIConRus) pp. 274–277. IEEE, (2019)
29. Alarab, I., Prakoonwit, S., & Nacer, M. I.: Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies, pp. 11–17 (2020)
30. Oad, A., Razaque, A., Tolemyssov, A., Alotaibi, M., Alotaibi, B., Zhao, C.: Blockchain-enabled transaction scanning method for money laundering detection. Electronics **10**(15), 1766 (2021)
31. Karasek-Wojciechowicz, I.: Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces. J. Cybersecurity 7(1), tyab004 (2021)
32. Park, K., Youm, H.Y.: Proposal for customer identification service model based on distributed ledger technology to transfer virtual assets. Big Data Cogn. Comput. **5**(3), 31 (2021)
33. Hughes, S. J.: 'Gatekeepers' are vital participants in anti-money-laundering laws and enforcement regimes as permission-less blockchain-based transactions pose challenges to current means to 'Follow the Money'. Indiana Legal Studies Research Paper, (408) (2019)
34. Jung, E., Le Tilly, M., Gehani, A.: Data mining-based ethereum fraud detection. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 266–273. IEEE (2019)
35. Lou, Y., Zhang, Y., & Chen, S.: Ponzi contracts detection based on improved convolutional neural network. In: 2020 IEEE International Conference on Services Computing (SCC) pp. 353–360. IEEE (2020)

36. Bian, L., Zhang, L., Zhao, K., Wang, H., Gong, S.: Image-based scam detection method using an attention capsule network. IEEE Access **9**, 33654–33665 (2021)
37. Chen, W., et al.: Sadponzi: Detecting and characterizing ponzi schemes in ethereum smart contracts. Proc. ACM Meas. Anal. Comput. Syst. **5**(2), 1–30 (2021)
38. Fan, S., Fu, S., Xu, H., Cheng, X.: Al-SPSD: Anti-leakage smart Ponzi schemes detection in blockchain. Inf. Process. Manage. **58**(4), 102587 (2021)
39. Yu, S., Jin, J., Xie, Y., Shen, J., & Xuan, Q.: Ponzi scheme detection in ethereum transaction network. In: International Conference on Blockchain and Trustworthy Systems pp. 175–186. Springer, Singapore (2021)
40. Jin, C., Jin, J., Zhou, J., Wu, J.: Heterogeneous Feature Augmentation for Ponzi Detection in Ethereum. Express Briefs, IEEE Transactions on Circuits and Systems II (2022)
41. Jin, C., Zhou, J., Jin, J., Wu, J., & Xuan, Q.: Time-aware metapath feature augmentation for ponzi detection in ethereum. arXiv preprint arXiv:2210.16863 (2022)
42. Tian, F. (2017, June). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In: 2017 International conference on service systems and service management pp. 1–6. IEEE (2017)
43. Galvez, J.F., Mejuto, J.C.: Future challenges on the use of blockchain for food traceability analysis TrAC. Trends Anal. Chem. **107**, 222–232 (2018)
44. Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R.: Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In: 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany) pp. 1–4. IEEE (2018)
45. Westerkamp, M., Victor, F., & Küpper, A.: Blockchain-based supply chain traceability: Token recipes model manufacturing processes. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1595–1602. IEEE (2018)
46. Salah, K., Nizamuddin, N., Jayaraman, R., Omar, M.: Blockchain-based soybean traceability in agricultural supply chain. IEEE Access **7**, 73295–73305 (2019)
47. Wang, Z., Wang, T., Hu, H., Gong, J., Ren, X., Xiao, Q.: Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. Autom. Constr. **111**, 103063 (2020)
48. Behnke, K.: Boundary conditions for traceability in food supply chains using blockchain technology. Int. J. Inf. Manage. **52**, 101969 (2020)
49. Shahid, A., Almogren, A., Javaid, N., Al-Zahrani, F.A., Zuair, M., Alam, M.: Blockchain-based agri-food supply chain: A complete solution. IEEE Access **8**, 69230–69243 (2020)
50. Tsai, F.C.: The application of blockchain of custody in criminal investigation process. Proc. Comput. Sci. **192**, 2779–2788 (2021)
51. Tian, Z., Li, M., Qiu, M., Sun, Y., Su, S.: Block-DEF: A secure digital evidence framework using blockchain. Inf. Sci. **491**, 151–165 (2019)
52. Kim, D., Ihm, S.Y., Son, Y.: Two-level blockchain system for digital crime evidence management. Sensors **21**(9), 3051 (2021)
53. Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y.: Blockchain-based electronic evidence storage and efficiency optimization. In: 2021 international conference on artificial intelligence and blockchain technology (AIBT) pp. 109–113. IEEE (2021)