Automated Monitoring and Anomaly Detection in Blockchain Based Networks Through Use of Complicated Event Processing

IJIMSR, Vol. 2, No. 2, (2024) 24.2.2.021

Swathi Ch
Department of Computer Science and Engineering
G Narayanamma Institute of Technology and Science
Hyderabad, Telanagan, India
Email: chswathi0508@gmail.com

Mohd Riyazuddin
Department of Computer Science and Engineering
Keshav Memorial Institute of Technology
Narayanguda, Hyderabad, Telanagan, India
Email: riyazuddin17@gmail.com

***Ramesh Cheripelli**
Department of Information Technology
Vidya Jyothi Institue of Technology
Hyderabad, Telanagan, India
Email: drrameshchit@vjit.ac.in

***Corresponding author**

Received 12th July 2024; Accepted 31st August 2024

KEYWORDS: Blockchain, Hyperledger Fabric, Anomaly, Complex Event Processing

Automated Monitoring and Anomaly Detection in Blockchain Based Networks Through Use of Complicated Event Processing

Swathi Ch
Department of Computer Science and Engineering
G Narayanamma Institute of Technology and Science
Hyderabad, Telangana, India
Email: chswathi0508@gmail.com

Mohd Riyazuddin
Department of Computer Science and Engineering
Keshav Memorial Institute of Technology
Narayanguda, Hyderabad, Telangana, India
Email: riyazuddin17@gmail.com

Ramesh Cheripelli
Department of Information Technology
Vidya Jyothi Institue of Technology
Hyderabad, Telangana, India
Email: drrameshchit@vjit.ac.in

ABSTRACT

Blockchain is a contemporary technology that promotes trust in the digital society by providing information with the qualities of immutability, traceability, and transparency. In addition to transactions, blocks, and events, blockchain networks generate copious amounts of logs that document and describe the data that traverses the network. It is imperative to monitor blockchain data from the off-chain world in order to detect any irregularities and mitigate the potential risks associated with the use of blockchain technology. The increased volume of daily transactions on blockchain networks has made it increasingly challenging to monitor these records in real time using off-chain tools since the beginning of 2018. This paper proposes an architecture that integrates complex event processing technologies with blockchain technology. The architecture is intended to be readily configurable, maintainable, and portable. This design was subjected to testing by utilizing extensive blockchain data that had already been publicly recorded on the Hyperledger Fabric networks. The results suggest that the proposed framework has the ability to autonomously detect a variety of blockchain network irregularities, thereby facilitating the analysis of blockchain data using off-chain platforms. the results and findings. Conclusions: Give brief concluding remarks on your outcomes.

KEYWORDS: Blockchain, Hyperledger Fabric, Anomaly, Complex Event Processing

1. INTRODUCTION

As a result of the rapid digitization of the globe and widespread access to Internet, there has been a significant increase in the number of people participating online in all aspects of life and business. In contrast to this, it became a great deal more difficult to keep track of all of the exchanges. This is one of the reasons why the blockchain technique should be implemented in order to keep data secure and up to date while also keeping a record of its history within the system. Conventional systems have a lack of transparency, make scaling challenging, and create a significant margin for error [1,2].

Securely propagating data from one participant to another, blockchain technology builds an ever-expanding list of immutable records called blocks and links them together to form a chain is shown in figure 1.

Peer nodes are used to symbolize the members within a network that is so extensive that it spans the entire globe. With this technique, organizations are able to reach a consensus on a single, dispersed source of truth so that they may work together. Upon validation via the consensus mechanism, transactions can be applied from any of the peers' copies of the ledger. In addition, the use of hashes to link blocks together makes the blockchain impervious to data manipulation [3,4].

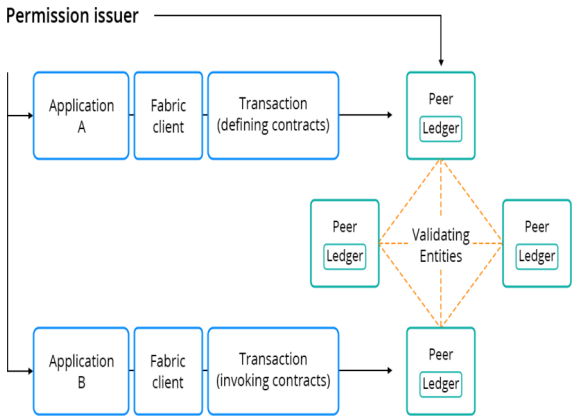


Figure 1: Blockchain system with multiple modules

2. HYPERLEDGER FABRIC

Hyperledger Fabric platform that is open-source and geared for usage in enterprise contexts overview is shown in figure 2. It has unique capabilities that set it apart from other prominent distributed ledger or blockchain platforms.[7,8]

One crucial distinction is that Hyperledger was founded within the Linux Foundation, an organization with a notable track record of fostering open-source initiatives through transparent governance, resulting in the development of robust, sustainable communities and flourishing ecosystems. The governance of Hyperledger is overseen by a varied Technical Oversight Committee (TOC), whilst the management of the Hyperledger Fabric project is carried out by a diverse group of maintainers from various companies. Hyperledger Fabric has received contributions from numerous developers across multiple organizations. [6,9]

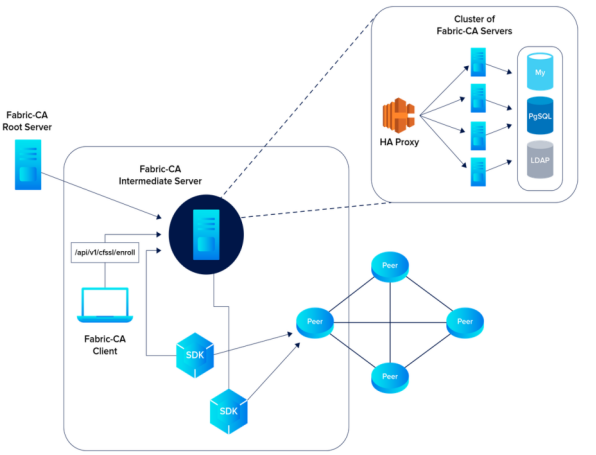
Fabric possesses a remarkably modular and adaptable structure, allowing for innovation, flexibility, and optimization across several industries. Consequently, majority of businesses already possess the necessary expertise to create smart contracts, eliminating the requirement for further instruction in a different programming language or domain-specific language (DSL).

The Fabric platform operates on a permissioned basis, ensuring that all players are identifiable and not anonymous. This guarantees that the participants are completely untrusted. This suggests that even if the participants harbor a certain degree of mistrust towards one another, such as being rivals in the same field, a network can still operate by implementing a governance framework that is built upon the current level of trust among the participants. This can be accomplished by procedures such as a legally binding agreement or a structured framework for resolving disputes.

A distinguishing characteristic of this platform is its capability to facilitate pluggable consensus mechanisms. This feature enables the platform to be readily customized to suit unique use cases and trust models. In situations when a single enterprise is utilizing it or when it is overseen by a trusted authority, implementing a completely byzantine fault tolerant consensus would be considered unnecessary and could have a detrimental effect on performance and throughput. [10,14]

Fabric can employ consensus methods that do not require a native cryptocurrency to incentivize costly mining or enable smart contract execution. By abstaining from utilizing a cryptocurrency, the platform can effectively eliminate certain high-risk attack vectors. Furthermore, the absence of cryptographic mining activities enables the platform to be deployed with comparable operational expenses to current distributed systems.

Fabric distinguishes itself from other platforms by its distinctive design elements, which enhance its exceptional performance in processing transactions and minimizing transaction confirmation delays. [11,13]



3. RELATED WORK

The literature on blockchain technology is substantial, encompassing a wide range of themes that include, but are not limited to, cloud computing, database systems, digital twins, educational technologies, interoperability, smart contracts, the internet of things (IoT), and the creation of electronic voting systems. [12] The privacy, cybersecurity, and system security of blockchain frameworks are all topics covered in numerous surveys.

Here we focus on the following research that seem to be more pertinent to the present effort, even though the aforementioned works do touch on anomaly detection and deanonymization to a lesser degree.

Musa et al. classed anomaly detection methods and kinds based on learning modes and methodologies, focusing on the fields of application. The domains of application encompassed medical research, image processing, industrial damage assessment, as well as intrusion and fraud detection systems. These techniques encompassed a broad spectrum of computational strategies. [15]

Chandola et al. created a fundamental framework for categorizing anomaly detection by integrating information-theoretic and spectral methodologies with current grouping methods. As a result, they meticulously delineated the benefits and drawbacks of each selected approach, providing a thorough study of the computational complexity for each method. They also established their classifications by utilizing specific assumptions and criteria to detect outliers. [16] Pourhabibi et al. developed a hierarchical framework to classify various methods used in fraud detection. This framework takes into account many criteria, including the types of networks and anomalies used. This framework specifically emphasizes the utilization of graph-based techniques for detecting anomalies. In addition, they delineated the obstacles present in the domain of fraud detection utilizing graph-based structures and furnished a catalogue of the most noteworthy ones.[18,19]

Hisham et al. assert that ensembles of classifiers can effectively tackle several vulnerabilities in blockchain frameworks, including security, abuse, cyber-attacks, criminal activities, and money laundering. The researchers highlighted the significance of the previously mentioned models in the process of analyzing data, which involves preparing and preprocessing the data. Their attention was directed on the strengths and shortcomings of these models in order to guarantee a methodical and dependable presentation. [20]

Despite blockchain's status as a frontrunner in decentralized application development, it has demonstrated some shortcomings in terms of smart contract and cryptocurrency security. Using data-mining models with well-defined metrics, criteria, and needs can effectively mitigate the aforementioned problems, especially with regard to the model's resilience. Some of these review articles go even farther, focusing on how abnormalities in blockchain networks can be discovered through data mining and machine learning. For instance, Li et al. distinguished between two main schools of thought when looking at the topic from a detailed perspective.[21,22]

There are two categories of methods those with a broad objective and no particular focus on anomalies, and those tailored to certain kinds of abnormalities. Each of the aforementioned groupings was further subdivided into multiple subgroups according to clearly stated criteria. The structure of each subgroup was described and the advantages and disadvantages of each subgroup were examined.

In the inductive methodology was used to study bitcoin security flaws. The main goal of the investigation was to determine which data mining algorithms had qualities that would make them possible to execute, considering the failures outlined before. The use of data mining techniques to identify outliers in blockchain settings was examined in with reference to specific features of these settings, including transparency and decentralization. Among the domains that were examined were healthcare, supply chain management, cryptocurrency, and finance. Looking at data mining models for blockchain anomaly detection from a different angle. In order to develop a generic approach to model creation, the authors used specific criteria to evaluate the corresponding robustness and performance. In order to achieve this goal, the writers engaged in a conversation regarding the ongoing issues, obstacles, and plans for future study.

4. NETWORK ANOMALIES IN BLOCKCHAIN

Blockchain technologies are vulnerable to unique attacks and challenges notwithstanding their benefits. Blockchain network attacks reduce its capital or popularity, lowering its market value.

The credibility of financial transactions is jeopardized by double-spending assaults, in which criminals

repeatedly spend the same cryptocurrency. A Bitcoin client may use the same Bitcoin in several transactions due to network latency in broadcasting pending payments. The 51% attack poses a further perilous predicament, wherein one or more entities acquire dominance over more than 50% of the network's mining power and subsequently alter transactions. Nevertheless, Sybil attacks, which entail the establishment of several fake identities or nodes by attackers in order to seize control over a major percentage of the network and disrupt consensus and transaction validation, are quite common. Sybil attacks are a type of cyberattack. Another significant vulnerability is known as eclipse attacks, in which malevolent nodes encircle a target node, granting them the ability to alter or selectively block transactions. When a group of miners attempt to gain unfair advantages over other miners, who adhere to ethical practices, it is referred to as "selfish mining." This behaviour poses a significant risk to the integrity of the blockchain network.

Re-entrancy and arithmetic overflows and underflows are two vulnerabilities that can be exploited by Ethereum smart contracts. These flaws can result in undesired outcomes and financial loss. Ponzi schemes that are based on blockchain technology exploit the confidence of customers by providing returns that are both unrealistic and detrimental to their financial situation.

5. ISSUES AND PLANS FOR THE FUTURE

Information mining tactics and blockchain technology's transformational power intersect in blockchain anomaly detection. As we investigate current methods and prepare for future advances, many difficulties and opportunities arise. Scalability is a major issue in blockchain anomaly detection. Traditional detection methods may struggle as blockchain data grows in volume and complexity. The heterogeneous blockchain structure has Scalability and complexity challenges [23]. Future research should combine graph learning and neural network methods to address scalability and complexity issues. Modeling blockchain networks using their structures is robust using graph learning. Using graph neural networks or LSTM can reveal complicated patterns and aberrant behaviors while avoiding scalability limits.

An interdependent association between data mining and network resilience is necessary to identify abnormal occurrences. Unsupervised learning and advanced deep learning algorithms can be employed to detect concealed irregularities, hence improving its integrity and dependability for upcoming initiatives.

Blockchain anomaly detection faces many risks. Anomaly detection can also be hampered by fake or deceptive blockchain data. Innovative mitigation solutions in ongoing research could focus on GenAI and adversarial learning to address these dangers. GenAI-powered anomaly detection (GADE) techniques may improve blockchain anomaly detection. Recent study suggests GADE approaches can enhance existing procedures. Address-user association on public blockchain networks could be handled via GADE. Unsupervised learning, especially data clustering, is effective for aggregating user addresses. GADE-based cluster analysis improves accuracy and scalability, making malicious user activity detection easier.

Recent research has explored how GenAI techniques can optimize the dynamic interplay between supervised and unsupervised operations. By integrating both paradigms, ensemble techniques powered by GADE have the potential to enhance the model's capacity to identify intricate blockchain irregularities. Combining Genetic Algorithm Driven Evolution (GADE) with unsupervised algorithms is expected to enhance the accuracy of anomaly identification, particularly in complex data sets [24].

Issue	Description	Impact	Potential Solution
Scalability	Resource-intensive monitoring of large-scale networks	High computational/storage requirements	Use of efficient algorithms, distributed monitoring
Data Privacy and Security	Balancing monitoring needs with user privacy	Compromise on user privacy	Privacy-preserving monitoring techniques
Accuracy of Anomaly Detection	Distinguishing between benign and malicious anomalies	False positives/negatives	Advanced machine learning models, contextual analysis
Real-Time Detection and Response	Implementing systems for real-time monitoring	Delays in detection and response	Real-time analytics and automated response systems
Interoperability	Integration across different blockchain platforms	Standardization difficulties	Development of interoperable standards and protocols
Complexity of Blockchain Data	Analyzing and interpreting complex blockchain data	Need for specialized tools and expertise	Development of user-friendly analysis tools

Table 1: Key Issues in Automated Monitoring and Anomaly Detection in Blockchain-Based Networks

6. CONCLUSION

This paper proposes a solution that involves an attacker who can trick their victim into believing that some of the blocks they got are legitimate and have already been approved by the mainstream chain. It is possible to achieve this result in blockchain-based applications by employing a wide variety of attacks, which can range from possessing 51% of the entire peer-to-peer network to utilizing the structure of the overlay network in order to eliminate the victim. Overlay networks, which are connections that form a graph upon which a distributed application is deployed, are utilized extensively by blockchain-based applications. This is due to the fact that overlay networks enable the deployment of network functionalities without requiring any modifications to the underlying infrastructure.

REFERENCES

[1] Hasan, M.; Rahman, M.S.; Janicke, H.; Sarker, I.H. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. 2024,

[2] D.J. Yaga, P.M. Mell, N. Roby, K. Scarfone, Blockchain Technology Overview, NIST Pubs 8202, NIST, Gaithersburg, MD, 2018, pp. 1–66.

[3] S. Farshidi, S. Jansen, S. España, J. Verkleij, Decision support for blockchain platform selection: Three industry case studies, IEEE Trans. Eng. Manage. 67 (4) (2020) 1109–1128,

[4] J. Boubeta-Puig, J. Rosa-Bilbao, J. Mendling, CEPchain: A graphical modeldriven solution for integrating complex event processing and blockchain, Expert Syst. Appl. 184 (Article 115578) (2021)

[5] Patel, V.; Pan, L.; Rajasegarar, S. Graph deep learning based anomaly detection in Ethereum blockchain network. Lect. Notes Comput. Sci. 2020, 12570, 132–148.

[6] Cheripelli R et al, Blockchain-Based System for the Secure Transfer of Assets,14th International Conference on Advances in Computing, Control, Telecommunication Technologies,2023, June,885-891

[7] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, G. Manco, A deep learning approach for detecting security attacks on blockchain, in: ITASEC, 2020, pp. 1–11.

[8] A. Hudaya, M. Amin, N.M. Ahmad, S. Kannan, Integrating distributed pattern recognition technique for event monitoring within the IoT-blockchain network,International Conference on Intelligent and Advanced System, ICIAS, 2018, pp. 1–6,

[9] G. Cugola, A. Margara, Complex event processing with T-REX, J. Syst. Softw. 85 (8) (2012) 1709–1728,

[10] Thallapelli, T. and Cheripelli, R. A Framework for E-Auction Scheme using Hyperledger Fabric,14th International Conference on Advances in Computing, Control, Telecommunication Technologies, 2023-June,1703-1709

[11] X. Xu, I. Weber, M. Staples, Architecture for Blockchain Applications, Springer International Publishing, Cham, Switzerland, 2019,

[12] Cheripelli R, New Challenges and its Security, Privacy Aspects on Blockchain Systems,14th International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2023-June,1491-1497

[13] X. Zheng, Y. Zhao, H. Li, R. Chen, D. Zheng, Blockchain-based verifiable privacypreserving data classification protocol for medical data, Comput. Stand. Interfaces 82 (2022) 103605,

[14] Cheripelli ,New Model to Store and Manage Private Healthcare Records Securely Using Block Chain Technologies, Communications in Computer and Information Science,2022,1550 CCIS,189-201 DOI: 10.1007/978-3-031-17181-9_15

[15] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, C. Yang, The blockchain as a decentralized security framework [future directions], IEEE Consum. Electron. Mag. 7 (2) (2018) 18–21

[16] M. Liu, Z. Zhang, W. Chai, B. Wang, Privacy-preserving COVID-19 contact tracing solution based on blockchain, Comput. Stand. Interfaces 83 (2022) 103643

[17] M. Du, Q. Chen, J. Xiao, H. Yang, X. Ma, Supply chain finance innovation using blockchain, IEEE Trans. Eng. Manage. 67 (4) (2020) 1045–1058

[18] C. Ramesh, Comparative analysis of applications of identity-based cryptosystem in IoT, Electronic Government, An International Journal, 2017, volume-13,314—323,2017.

[19] L.N. Sánchez-Morales, G. Alor-Hernández, V.Y. Rosales-Morales, C.A. CortesCamarillo, J.L. Sánchez-Cervantes, Generating educational mobile applications using UIDPs identified by artificial intelligence techniques, Comput. Stand. Interfaces 70 (2020) 103407

[20] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, A blockchain-empowered crowdsourcing system for 5G-enabled smart cities, Comput. Stand. Interfaces 76 (2021) 103517

[21] J. Rosa-Bilbao, J. Boubeta-Puig, RectorDApp: Decentralized application for managing university rector elections, in: 2021 IEEE International Conference on Service-Oriented System Engineering, SOSE, 2021, pp. 161–165

[22] J. Boubeta-Puig, G. Ortiz, I. Medina-Bulo, MEdit4CEP: A model-driven solution for real-time decision making in SOA 2.0, Knowl.-Based Syst. 89 (2015) 97–112

[23] R. Akkaoui, Blockchain for the management of Internet of things devices in the medical industry, IEEE Trans. Eng. Manage. (2021) 1–12

[24] A. Busse, J. Eberhardt, S. Tai, EVM-Perf: High-precision EVM performance analysis, in: 2021 IEEE International Conference on Blockchain and Cryptocurre