2025 International Conference on Advanced Mechatronics and Intelligent Energy Systems

Blockchain¡¯s Secure Applications in Healthcare, Internet of Things, and Supply Chain: Challenges and Prospects

AIPCP25-CF-AMIES2025-00108 | Article

Blockchain's Secure Applications in Healthcare, Internet of Things, and Supply Chain: Challenges and Prospects

Yalun Li

Computer Science, Hubei University of Technology, Wuhan, China

2310300727@hbut.edu.cn

Abstract. Blockchain has been recognized as an auspicious decentralized ledger technology, offering immutability, transparency, and trust without centralized intermediaries. The study conducts an extensive survey on blockchain security research across three key application domains, including healthcare, Internet of Things (IoT), and supply chain management. First, blockchain fundamentals are introduced, including consensus mechanisms and smart contracts, followed by a taxonomy of attack vectors. Next, domain-specific cases are examined. In the medical domain, techniques such as Long Short-Term Memory (LSTM)-based Sybil attack detection and smart contract-based access control are evaluated. In IoT environments, solutions including lightweight blockchain architectures and decentralized reputation mechanisms are explored. In supply chains, machine learning-based intrusion detection systems and threat modeling frameworks are discussed. The discussion highlights current limitations such as deep learning models struggling with scalability in healthcare, the synchronization and device heterogeneity challenges faced by IoT deployments, and the interoperability and data format inconsistencies encountered in supply chains. Future prospects include distributed deep learning for large-scale model training, lightweight consensus protocols for resource-constrained environments, AI-powered anomaly detection, and hybrid blockchain-edge computing architectures. By synthesizing existing research and mapping open problems, this review equips practitioners and researchers with a thorough grasp of blockchain security's current state and future directions.

INTRODUCTION

Blockchain technology, commonly referred to as a decentralized and unchangeable ledger system, eliminates the need for centralized intermediaries. It also makes use of consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) to ensure data integrity. As a result, it is becoming a revolutionary paradigm that aims to enhance trust in digital transactions. Blockchain is widely utilized in areas like finance, medical and Internet of Things (IoT) due to these advantages. In the IoT, its decentralized features address key challenges such as device authentication, secure data sharing, and access control. However, despite blockchain's claimed security guarantees, it remains vulnerable to various attacks. With the spread of technology, attackers continuously find new complex attacks, exploiting consensus mechanisms, smart contracts and network layer vulnerabilities, thereby heightening the risk even in IoT devices with limited resources. Understanding these attack vectors along with their classification, evolution, and situational adaptation has become a vital and urgent research frontier.

The evolution of blockchain security research has a close connection with its technical landmarks as well as the challenges it faces from adversaries. The fundamental principles of blockchain came into being in 2008 with the Bitcoin protocol put forward by Nakamoto [1], which introduced PoW to mitigate double-spending and establish decentralized consensus. In the early stages, the research mainly focused on making improvements to the consensus mechanisms, such as the Ethereum framework proposed by Buterin in 2015 [2], which expanded blockchain applications from cryptocurrencies to programmable transactions by introducing smart contracts. This initial work laid down the theoretical groundwork for the application of blockchain in multiple fields. At the same time, however, it also exposed potential vulnerabilities in its decentralized architecture, prompting adversaries to exploit its security flaws. With the popularity of blockchain technology, the types of attacks are gradually systematized. Scholars have

systematically classified blockchain attacks into three categories: protocol layer attacks, application layer exploitation, and hybrid threats.

In protocol-layer attacks, Eyal and Sirer were the pioneers who came up with the concept of selfish mining. They demonstrated precisely how attackers could obtain unfair rewards by deliberately withholding blocks in a strategic manner. This, in turn, posed a challenge to the traditional assumption of an "honest majority" within the blockchain context [3]. At the application layer, Atzei and others carried out a detailed dissection of the reentrancy attack that took place during Ethereum's DAO incident. They laid emphasis on the crucial flaws present in the logic of smart contracts [4]. Regarding hybrid threats, Rosenfeld put forward the Block Withholding Attack (BWH). He revealed the ways in which malicious miners could undermine mining pools [5]. The research on blockchain attacks has now extended beyond the financial sector and has reached into critical areas such as healthcare and the Internet of Things (IoT). In the healthcare, Hasan and his colleagues analyzed risks of data poisoning attacks in blockchain-based vaccine supply chains, like Pfizer's COVID-19 tracking system. They demonstrated that tampering with temperature logs could invalidate vaccines [6]. In a similar vein, within the IoT domain, Obaidat and others delved into the impact of Sybil attacks on IoT networks. They illustrated how malicious nodes have the capacity to disrupt the network topology as well as the efficiency of resource-sharing through the blockchain-based consensus mechanisms, as indicated in [7]. Moreover, Sharma and his team examined how blockchain can enhance IoT security at the application layer by countering Sybil attacks through cryptographic techniques and decentralized validation processes [8]. In recent years, the complexity of blockchain attacks has gradually increased. At the same time, blockchain has witnessed widespread adoption across diverse domains, including healthcare, IoT, and supply chain. Consequently, carrying out a systematic review of the various attack types, cross-domain cases, and the emerging defense mechanisms is essential to guide future research and practical applications.

The rest of the paper is arranged in the following way. First, Section 2 will cover some blockchain fundamentals, including consensus mechanism and blockchain attacks, and further examine the taxonomy of blockchain attacks and its application in different situations such as IoT, medical and supply chain. In addition, current challenges in the field and its future direction will be discussed in Section 3. Finally, Section 4 summarizes the review, discusses the key findings and implications for researchers and practitioners.

BLOCKCHAIN FUNDAMENTALS AND ATTACK APPLICATIONS ACROSS DOMAINS

Blockchain Preliminaries

Blockchain technology, often hailed as a revolutionary advancement in the digital age, is essentially a decentralized, distributed ledger that records transactions across multiple nodes in a secure and immutable manner. The core idea of blockchain dates back to the work of Haber and Stornetta, who proposed a method for timestamping digital documents to ensure their integrity [9]. However, it was not until the advent of Bitcoin by Nakamoto that blockchain gained widespread attention [1]. The structure of blockchain typically consists of a chain of blocks, each containing a cryptographic hash of the previous block, a timestamp, and transaction data. This structure ensures the integrity and security of the ledger.

Blockchain attacks can be broadly classified into several categories based on their nature and target. First, Sybil Attacks involve an attacker creating multiple fake identities to disrupt the consensus process. Second, 51% Attacks occur when an attacker gains control of the majority of the network's computational power to alter transaction records. Third, Phishing Attacks exploit human vulnerabilities by deceiving users into revealing sensitive information through fraudulent websites or emails. In addition, Routing Attacks involve manipulating routing protocols to intercept or redirect data packets, particularly related to IoT environments. Denial-of-Service (DoS) Attacks overwhelm the network with traffic, making it impossible for legitimate transactions to be processed. Finally, Double-Spending Attacks involve an attacker spending the same digital asset twice, thereby defrauding the system. These attack types highlight the diverse methods attackers use to exploit vulnerabilities of blockchain systems.

Smart contracts, self-executing contracts with the terms directly written into code, are another integral part of blockchain technology, enabling automated and transparent transactions without intermediaries. Consensus mechanisms, such as PoW and PoS, play an important role in maintaining the integrity of blockchain networks. Understanding these fundamental components and attack types is essential for analyzing the security challenges and potential solutions in various application domains.

Blockchain Attacks in the Medical Domain

Sybil Attack Mitigation in EHR Systems

Alghofaili and others proposed a blockchain-based trust model for Electronic Health Records (EHRs) using deep Long Short-term Memory (LSTM) to detect Sybil attacks. Their framework dynamically evaluates node reputation scores and achieved 91% detection accuracy in simulated medical networks. The method involves training an LSTM model to analyze node behavior patterns and assign reputation scores, thereby identifying malicious nodes [10].

Data Poisoning in Pharmaceutical Supply Chains

Hammi and others put forward a 'Bubbles of Trust' model which is based on blockchain for the purpose of alleviating data poisoning attacks within vaccine transportation chains. This particular solution makes use of distributed identity authentication along with dynamic data hash verification so as to lessen the likelihood of data being tampered with. In a simulated setting, this approach managed to attain an abnormal data detection rate of 89% [11].

Phishing via Smart Contract Exploits

Kumar and others put forward a blockchain-driven Sybil Secure Data Transmission (SSDT) framework meant for smart city healthcare applications. This framework scored the reputation of nodes dynamically and verified their identities by means of Zero-knowledge Proofs (ZKP). In doing so, it managed to prevent 87% of the fraudulent access requests. The method entails a multi-layered authentication process, which is designed to make sure that only legitimate nodes have the ability to access the sensitive medical data [12].

Blockchain Attacks in the IoT Domain

Eclipse Attacks on Edge Nodes

Dorri and his colleagues put forward a lightweight blockchain-SDN architecture for countering eclipse attacks within IoT networks. Their model managed to cut down node isolation incidents by as much as 78% in the context of smart home deployments. This was achieved by decentralizing traffic validation through ONOS controllers. The method entails distributing the responsibilities of traffic validation among multiple nodes so as to avoid a single point of failure [13].

Sybil Attacks on Resource-Constrained Devices

Sybil attacks pose a threat to IoT-blockchain systems as they flood the networks with fake identities. Obaidat and others put forward a dual defense mechanism. The Proof of Physical Work (PoPW) requires each device to solve cryptographic puzzles that are energy-bound, which makes the creation of Sybil identities rather costly. Meanwhile, a decentralized reputation system isolates malicious nodes by means of behavioral scoring. Their testbed using Raspberry Pi managed to achieve a 92% Sybil detection rate within 3 to 5 consensus rounds [7].

Sybil Attack Detection Using Deep LSTM

Alghofaili and others put forward a blockchain-centered trust model for IoT systems with the aim of detecting Sybil attacks. The method combines a deep LSTM network to assess node reputation scores in a dynamic manner and spot malicious nodes. The framework trains an LSTM model to analyze the behavioral patterns of nodes and then assigns reputation scores according to these patterns. In the simulated IoT networks, this approach managed to attain a detection accuracy of 91%. By making use of this method, IoT systems are able to defend against Sybil attacks effectively, thereby enhancing both the robustness as well as the credibility of IoT systems [14].

Blockchain Attacks in the Supply Chain Domain

Data Poisoning Attack Analysis in Blockchain-Enabled Supply Chain Networks

Butt and his colleagues put forward a machine learning-based IDS for the purpose of analyzing data poisoning attacks within blockchain-enabled supply chain networks. The study carried out experimental evaluations on random label flipping attacks as well as distance-based label flipping attacks, which were directed at models such as logistic regression, random forest, SVC, XGB, and an eight-layer neural network. By making use of the KDDCUP’99 dataset, the research made an assessment of the model performance under three different scenarios, namely, the scenario where there was no attack, the scenario with random label flipping (featuring 20% randomness), and the scenario involving distance-based label flipping (with a 0.5 threshold) [15].

Threat Modeling for Blockchain-Based Supply Chain Security

Al-Farsi and others worked out a threat model meant for supply chain management systems that are based on blockchain. Their focus was on aspects like transparency, privacy, as well as traceability. They sorted attacks into two types, namely the computational type and the communication type. Through an analysis of the existing solutions both in the academic field and in the industrial realm, they spotted certain gaps. For instance, there was a lack of sufficient transparency and also a deficiency in context awareness. The study put forward a suggestion that business process information and communication infrastructure should be integrated. By doing so, it would be possible to boost the security level. This would then allow the systems to detect threats and implement policies in a more effective manner [16].

Lightweight Machine Learning for Cyber-Attack Detection

Ismail and others put forward a blockchain-facilitated industrial supply chain security architecture that incorporates lightweight Machine Learning (ML) for the purpose of detecting cyber-attacks. They made use of the WUSTL-IIoT-2021 dataset and dealt with its imbalance by means of RandomUnderSampler. Feature selection was carried out through the utilization of Mutual Information (MI) and Extra-trees (ET) so as to lower the dimensionality. A variety of ML techniques, such as Naive Bayes, Random Forest, as well as ensemble methods like Stacking and Catboost, were appraised. Stacking attained the highest level of accuracy, whereas Catboost demonstrated the best precision. This particular approach effectively strikes a balance between performance and resource utilization within IIoT environments [17].

DISCUSSION

Limitations and Challenges

The combination of blockchain technology within the healthcare, Internet of Things (IoT), and supply chain fields has shown considerable potential for bolstering security, making things more transparent, and building trust. Nevertheless, each of these domains encounters distinct challenges that impede its broad acceptance.

Medical Domain

One notable limitation is the scalability of blockchain-based threat detection systems in complex healthcare environments, accompanied by limited real-world prototyping. While Alghofaili and others proposed an LSTM-based framework capable of detecting Sybil attacks in medical networks with over 90% accuracy, such deep learning models demand substantial computational resources, which may not be feasible in all healthcare infrastructures, particularly in low-resource settings [10]. Moreover, on the one hand, it is believed that conceptual models such as the “Bubbles of Trust” framework for vaccine logistics demonstrate promising abnormal data detection rates in simulations [11]. On the other hand, the vast majority of proposals remain at the proof-of-concept or small-scale pilot stage, with a limited number of empirical studies or real-world implementations to evaluate their interoperability, deployment complexity, or operational robustness.

IoT Domain

The IoT environment brings about distinctive challenges on account of the restricted computational capacity of edge devices. Solutions such as Proof of Physical Work (PoPW) and the method of behavioral reputation scoring do enhance the detection of Sybil attacks within constrained IoT nodes. However, their energy consumption and latency demands can turn out to be quite restrictive when implemented on a large scale [7]. Additionally, decentralized defense mechanisms like the one put forward by Dorri and his colleagues remain reliant on network synchronization and the reliability of the controller. And these aspects can be undermined when subjected to targeted Eclipse attacks [13].

Supply Chain Domain

Blockchain's integration within industrial supply chains frequently gets hindered because of the complex requirements regarding interoperability as well as the heterogeneity of data. The IDS that is based on machine learning and was proposed by Butt et al., though it proves to be effective when it comes to countering data poisoning, it presumes the existence of structured datasets and known attack patterns [15]. However, in the real world, supply chains have to handle highly dynamic data flows and quite often there is a lack of the labeled data which is essential for supervised learning. Moreover, Ismail and others underlined the hardship in achieving a balance between performance and resource efficiency when ML models are being deployed in IIoT environments [17].

Future Prospects

In response to these limitations, several research and development directions can be explored to enhance blockchain’s resilience and usability across the three domains.

Medical Domain

In order to enhance the scalability within threat detection systems, future research might look into the combination of distributed training and blockchain. Distributed training makes it possible for numerous institutions like hospitals and clinics to work together in training models while safeguarding data privacy. In this way, it lessens the computational load on each individual entity.

IoT Domain

Lightweight consensus mechanisms such as Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) should be further optimized for IoT. These mechanisms require significantly less computation than traditional PoW and can be tailored for hierarchical IoT architectures. Furthermore, hybrid architectures integrating blockchain with edge computing nodes could offload computational burden from endpoint devices, enhancing security without degrading performance [13].

Supply Chain Domain

Future supply chain systems stand to gain from the integration of blockchain along with real-time anomaly detection that makes use of unsupervised machine learning, which doesn't call for pre-labeled data. This would heighten the adaptability in the face of unknown attack vectors and supply chain disruptions. Moreover, when blockchain is combined with digital twin technology, it could present end-to-end traceability, with the digital replica of a product's lifecycle on-chain being continuously verified via IoT sensors [16]. Also, industry-specific lightweight blockchains might lessen the complexity and cut down on the cost during large-scale deployments, as Ismail et al. have indicated [17].

CONCLUSION

This paper put forward a comprehensive review of blockchain technology and its application in three domains, which consist of healthcare, IoT, and supply chain management. The security challenges, attack vectors, and emerging defense mechanisms associated with blockchain in these sectors were examined. Through analyzing a variety of

research studies, this review identified the crucial vulnerabilities in blockchain systems, such as Sybil attacks, data poisoning, and phishing threats, and discussed their impact on the reliability and efficiency of blockchain networks.

The author explored the current challenges faced in each domain. These challenges encompass issues related to scalability, intricacies of integration, as well as resource limitations. Additionally, promising future directions were highlighted, such as the integration of advanced machine learning models, advancing more efficient and resource-friendly consensus protocols, and the adaptation of blockchain with emerging technologies like edge computing and IoT sensors. Although blockchain holds substantial potential for enhancing security and transparency, continued research and innovation remain essential to tackle the remaining drawbacks. In the future, further studies could center on improving blockchain's adaptability and resilience in resource-constrained environments and refine its integration into real-world applications.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" (2008).
2. V. Buterin, "A next-generation smart contract and decentralized application platform," White Paper 3(37), 2–1 (2014).
3. I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in Proc. Int. Conf. on Financial Cryptography and Data Security, Springer, 436–454 (2014).
4. N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in Int. Conf. on Principles of Security and Trust, Springer, Berlin, Heidelberg, (2017).
5. M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," arXiv preprint arXiv:1112.4980 (2011).
6. A. Musamih, et al., "Blockchain-based solution for distribution and delivery of COVID-19 vaccines," IEEE Access, 99 (2021).
7. M. A. Obaidat, et al., "Exploring IoT and blockchain: A comprehensive survey on security, integration strategies, applications and future research directions," Big Data Cogn. Comput. 8(12), 174 (2024).
8. G. Sharma, et al., "A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open issues," Electronics 10(19), 2365 (2021).
9. S. Haber and W. S. Stornetta, "How to time-stamp a digital document," J. Cryptol. 3(2), 99–111 (1991).
10. Y. Alghofaili and M. A. Rassam, "A dynamic trust-related attack detection model for IoT devices and services based on the deep long short-term memory technique," Sensors 23(8), 3814 (2023).
11. S. Datta, et al., "Authentication and privacy preservation in IoT-based forest fire detection by using blockchain – a review," in Proc. 4th Int. Conf. on Internet of Things and Connected Technologies (ICIoTCT), Springer, (2019).
12. S. Kumar, A. K. Das, and D. Sinha, "Blockchain-based Sybil-secure data transmission (SSDT) IoT framework for smart city applications," in Evolution in Computational Intelligence: Frontiers in Intelligent Computing: Theory and Applications (FICTA 2020), Vol. 1, Springer Singapore, (2021).
13. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in Proc. 2nd Int. Conf. on Internet-of-Things Design and Implementation (IoTDI), (2017).
14. A. Dixit, A. Trivedi, and W. W. Godfrey, "A survey of cyber attacks on blockchain-based IoT systems for Industry 4.0," IET Blockchain 4(4), 287–301 (2024).
15. U. J. Butt, et al., "Predicting the impact of data poisoning attacks in blockchain-enabled supply chain networks," Algorithms 16(12), 549 (2023).
16. S. Al-Farsi, M. M. Rathore, and S. Bakiras, "Security of blockchain-based supply chain management systems: Challenges and opportunities," Appl. Sci. 11(12), 5585 (2021).
17. S. Ismail, et al., "A comparative study of lightweight machine learning techniques for cyber-attacks detection in blockchain-enabled industrial supply chain," IEEE Access (2024).