# Blockchain-Based Approaches for Network Security Enhancement: Mechanisms, Applications, and Future Directions

Chenning Li

Xi'an Jiaotong University, Xi'an, Shaanxi, China

helenlee1811@163.com

**Abstract.** Traditional network security mechanisms, including firewalls, intrusion detection systems, and cryptographic schemes, have become insufficient in combating increasingly sophisticated cyberattacks. The emergence of decentralized and large-scale network environments, such as the Internet of Things (IoT) and cloud computing, has further complicated the protection of data integrity, privacy, and trust management. In this context, blockchain technology provides a new paradigm for enhancing network security through decentralization, immutability, and cryptographic consensus mechanisms. This paper explores the achievements and future prospects of blockchain applications in network security based on an extensive review of recent studies, which are mainly published in IEEE, Springer, and Elsevier, as well as experimental case studies from real-world blockchain-based security frameworks. It introduces the principles of blockchain and the challenges inherent in current network security systems. Then, it investigates how blockchain has been effectively utilized in distributed denial-of-service (DDoS) mitigation, threat intelligence sharing, and secure data sharing in IoT environments. Existing challenges of blockchain-based applications are also discussed, including scalability, interoperability, and energy efficiency. Furthermore, it evaluates potential directions for future research and development. The findings suggest that integrating blockchain into network security infrastructure can significantly improve transparency, resilience, and trustworthiness in digital ecosystems.

**Keywords:** Blockchain; Network Security; DDoS Mitigation; Threat Intelligence Sharing; IoT Security.

## 1. Introduction

The exponential growth of digital connectivity has made modern networks increasingly vulnerable to cyber threats. Conventional security mechanisms, such as firewalls, signature-based intrusion detection systems, and encryption protocols, are no longer sufficient to counter advanced and continuously evolving attacks [1]. These traditional methods often depend on centralized architectures that suffer from single points of failure, slow response times, limited adaptability to new attack patterns, and high maintenance costs [2]. Moreover, the proliferation of the Internet of Things (IoT), cloud computing, and mobile devices has introduced a massive number of potential attack vectors that further complicate network defense. In particular, traditional detection and mitigation methods lack adaptability to dynamic threats. Machine learning–based models may fail to detect zero-day attacks or evolving threat signatures [3]. As a result, security systems struggle to respond in real time, leaving organizations exposed to severe damage to the confidentiality, integrity, and availability of data. Blockchain technology offers a novel approach to strengthening network security. Its decentralized structure, cryptographic verification, and consensus mechanisms provide trust and transparency without relying on intermediaries. Through distributed ledgers, smart contracts, and immutable audit trails, blockchain can facilitate secure data exchange and collaborative threat mitigation across diverse entities. Recent research has demonstrated the potential of blockchain in mitigating distributed denial-of-service (DDoS) attacks, improving cross-organizational threat intelligence sharing, and ensuring data integrity in IoT systems. This paper aims to explore the mechanisms, applications, challenges, and future prospects of blockchain integration into network security systems, providing an in-depth perspective on how this technology can improve the

cybersecurity landscape. This study synthesizes findings from over 60 peer-reviewed works published between 2019 and 2025 to evaluate blockchain's role in strengthening network security systems.

## 2. Blockchain Technology Overview

Blockchain is a decentralized digital ledger that records transactions across a distributed network of nodes in a transparent, immutable, and tamper-resistant manner [4]. Each record, known as a block, contains a cryptographic hash of the previous block, a timestamp, and transaction data, thereby forming a secure and continuous chain. Since its introduction through Bitcoin in 2009, blockchain technology has evolved beyond cryptocurrencies to encompass diverse domains such as supply chain management, healthcare, finance, and network security [5]. A blockchain is typically managed by a peer-to-peer network that facilitates internode communication as well as validating new transactions. In this decentralized system, in order to create the next block of verified transactions and append to the existing blockchain, various consensus algorithms are proposed. Some of the widely used algorithms are proof of work (PoW), proof of stake (PoS), and practical Byzantine fault tolerance (PBFT). In PoW, participants are required to solve complex mathematical puzzles, and the first successfully computed node will be verified by the other nodes and selected as an authorized node to add the transaction to the block. In PoS, participants are allowed to validate transactions and create new blocks based on their ownership or stake in a cryptocurrency. Therefore, users possessing more currency can have the authority to add transactions to the blockchain. PBFT ensures that a distributed network can reach consensus even when up to one-third of the nodes are faulty [6]. Blockchain systems can be classified into three main types: public, private, and consortium (or federated) blockchains. Public blockchains, such as Bitcoin and Ethereum, are open to anyone, ensuring transparency and decentralization, but often suffer from scalability issues. Private blockchains restrict access to authorized participants, offering greater control and performance, suitable for enterprise use. Consortium blockchains combine the benefits of both, enabling multiple organizations to collaboratively maintain the ledger while retaining a degree of privacy and efficiency [6]. The intrinsic features of blockchain—immutability, transparency, traceability, and decentralization—make it a promising foundation for addressing critical security challenges in modern networks. By eliminating the need for a central authority and providing verifiable audit trails, blockchain enhances trust and resilience against manipulation and unauthorized access, thus presenting a strong potential for improving cybersecurity infrastructure.

## 3. Problems in Network Security

Modern network environments face an array of security challenges that traditional systems struggle to address effectively. Among the most critical of these, distributed denial-of-service (DDoS) attacks, IoT vulnerabilities, and cloud security risks are particularly significant. To begin with, DDoS attacks overwhelm network resources by flooding them with illegitimate traffic, rendering services inaccessible to legitimate users. In centralized architectures, distinguishing between valid and malicious requests is difficult. The massive scale of modern DDoS attacks—often reaching terabit-per-second traffic volumes—poses severe risks to service providers. The 2016 Mirai botnet incident exemplifies this problem, in which compromised IoT devices launched attacks exceeding 1 Tbps against providers such as Dyn and OVH, disrupting major internet services [7]. In addition to DDoS threats, the increased number of connected devices in IoT poses several challenges, for instance, to effectively handle the enormous amounts of data, interoperability among various hardware and software platforms, challenges related to Big data management, privacy and provenance, mobility management and handover, and privacy and security challenges [8]. Moreover, physical access and supply chain tampering create additional vectors for compromise. Attackers can exploit these weaknesses to infiltrate networks, exfiltrate data, or disrupt critical services. Furthermore, cloud

infrastructures, though efficient and scalable, expand the attack surface by distributing resources across multiple locations. Misconfigurations, insider threats, and API vulnerabilities increase the risk of data breaches. Additionally, traditional security monitoring tools often lack visibility across dynamic, multi-cloud environments [9]. Overall, the evolving threat landscape demands real-time coordination and authentication among stakeholders—network operators, Internet service providers, and mitigation providers—to effectively counter large-scale attacks. Blockchain, with its decentralized trust model and immutable records, offers a potential foundation for achieving secure, collaborative, and transparent network defense.

## 4. Blockchain for Network Security: Mechanisms

Overall, blockchain's decentralized architecture, consensus algorithms, and smart contracts make it suitable for building resilient network security frameworks [10]. In a blockchain-based total network, data is sent through multiple nodes, and each block is encrypted, making it hard for hackers to gain access to and manipulate information. And with smart contracts, which are self-executing programs designed to automatically enforce agreements when predefined conditions are met, admission to records may be controlled and confined, reducing the chance of insider assaults and ensuring network security. In a blockchain-based network, the consensus mechanism filters out fake requests, substantially lowering the threat of DDoS assaults. Because data and services are spread across thousands of computers, there is no central server to overwhelm. An attacker would need to take down the entire network, which is practically impossible. Once a threat, such as a malicious IP address, is posted to the blockchain, it cannot be altered or deleted. This makes the information trustworthy. Moreover, smart contracts can automatically and instantly share new threat data with all members, enhancing the speed and effectiveness of defenses. In the context of IoT, sensors can record a "fingerprint" of their data on the blockchain, proving the data is original and hasn't been changed. Smart contracts can automatically sell or grant access to this data. Collectively, these blockchain-native mechanisms establish a foundational layer of trust and automation that can be strategically leveraged to address a wide spectrum of network security challenges.

## 5. Applications

Blockchain's decentralized architecture enables multiple innovative applications in network defense. Its immutability, traceability, and distributed trust mechanisms are particularly well-suited for dealing with cyber threats that exploit central points of failure. This section elaborates on how blockchain can be applied to mitigate DDoS attacks, facilitate network threat intelligence sharing, and enhance data security in IoT ecosystems. In protecting against DDoS attacks, blockchain enables distributed coordination for DDoS mitigation through decentralized rule sharing and verification. By storing routing policies, threat intelligence, and filtering rules on a shared ledger, multiple Internet service providers (ISPs) can collaborate without depending on a single central authority [6]. Smart contracts can automate the enforcement of mitigation strategies, ensuring accountability and transparency among participants. Using network-level mitigation strategies, DDoS mitigation focuses on decentralizing traffic validation and filtering. Instead of relying on a centralized scrubbing center, blockchain nodes distributed across the network collectively authenticate, verify, and log packet metadata using consensus protocols. Routers or edge gateways can function as blockchain nodes that record summarized flow information, enabling real-time verification and anomaly detection. Smart contracts automate rules that trigger distributed filtering mechanisms when abnormal traffic is detected. Near-attack domain mitigation aims to detect and neutralize DDoS traffic close to its origin. Blockchain-based systems deployed near the attack domain utilize distributed verification and reputation scoring to identify malicious nodes early. Each node participating in traffic forwarding records its activity and reputation score on the blockchain. This early filtering prevents malicious traffic from propagating to the target. Near-victim mitigation focuses on filtering attack traffic closer

to the target. Blockchain nodes at the perimeter authenticate and prioritize legitimate requests. Smart contracts enforce access control rules, and immutable logs support forensic analysis. Although this method provides fine-grained control, it is often combined with near-source filtering to reduce congestion. Hybrid mitigation strategies integrate both near-source and near-victim strategies. The blockchain acts as a coordination layer linking distributed mitigation nodes. Consensus mechanisms ensure all nodes share consistent attack information and mitigation rules, enabling proactive defense across networks.

In addition to DDoS protection, blockchain also facilitates decentralized threat intelligence sharing, which is vital for proactive cybersecurity. Traditional threat intelligence sharing among organizations is often hindered by issues of trust, data integrity, and privacy. Blockchain provides a secure and immutable platform for recording and exchanging cyber threat intelligence (CTI). Each participating organization operates a node that submits verified indicators of compromise (IoCs) to the ledger. These entries are timestamped, digitally signed, and immutable, ensuring authenticity and preventing tampering [11]. Smart contracts can also establish incentive-based ecosystems for sharing intelligence. Contributors receive reputation points or cryptocurrency tokens when their shared intelligence assists in detecting or preventing attacks. This economic model, as demonstrated in platforms like PolySwarm, fosters active participation from researchers and organizations while ensuring data reliability and quality [12]. Blockchain's decentralized nature thus enables real-time, cross-domain collaboration in detecting and responding to cyber threats. Furthermore, blockchain can enhance data sharing security in the Internet of Things (IoT) systems. It requires high security to apply this technology to data processing systems because more data must be saved in cloud monitoring systems. It is essential to include data blocks that, under any circumstance, other external users cannot understand [13]. Blockchain ensures data integrity by allowing each IoT device to store cryptographic hashes of its data on the ledger, verifying authenticity without exposing raw data. Smart contracts enable fine-grained access control, permitting only authorized entities to read or modify data based on predefined rules. Consortium blockchains are particularly suitable for industrial IoT environments, enabling multiple enterprises to share operational data securely. Credit-based consensus mechanisms can enhance trust among devices and organizations. Additionally, blockchain-based data provenance ensures traceability and accountability across complex IoT ecosystems. By decentralizing control and encrypting transactions, blockchain effectively mitigates the risks of data tampering, unauthorized access, and single-point failures in IoT applications [14].

## 6. Challenges and Limitations

Despite its potential, the integration of blockchain into network security faces several technical and operational challenges. Scalability remains a major concern. Public blockchains, such as Bitcoin and Ethereum, experience limited throughput and high latency, rendering them unsuitable for real-time security operations that demand rapid response. Solutions such as sharding and off-chain processing are under development but have not yet reached full maturity. Energy consumption poses another challenge, particularly for Proof of Work–based systems, which require substantial computational power. The associated carbon footprint and operational costs are significant barriers to large-scale adoption. More energy-efficient consensus mechanisms, like Proof of Stake or Proof of Authority, offer potential alternatives but may compromise decentralization to some extent. Interoperability and standardization also hinder blockchain's integration across diverse networks. Security infrastructures vary widely between organizations, and without standardized protocols, blockchain-based systems may struggle to achieve cross-domain compatibility. Furthermore, privacy concerns arise from blockchain's transparency—while immutability ensures integrity, it may inadvertently expose sensitive data if not properly managed. Finally, regulatory and governance issues remain unresolved. Jurisdictions differ in their legal interpretations of decentralized technologies, which complicates the deployment of blockchain-based security frameworks across

borders. Addressing these limitations will require continued research, innovation in protocol design, and collaboration between policymakers and industry leaders.

## 7. Future Directions and Opportunities

Looking ahead, blockchain is expected to play a pivotal role in shaping the future of network security infrastructures, addressing current limitations while enabling novel applications across technical, operational, and policy domains. As cyber threats continue to grow in scale and sophistication, decentralized trust and automated verification mechanisms will become essential components of resilient defense systems. Future blockchain-based architectures will likely integrate with artificial intelligence (AI) and machine learning (ML) to enable predictive analytics, anomaly detection, and automated response mechanisms. Advancements in layer-2 scaling solutions and cross-chain interoperability are expected to overcome current performance bottlenecks, allowing blockchain networks to handle the high transaction volumes required in security operations. Meanwhile, the adoption of energy-efficient consensus mechanisms, such as Delegated Proof of Stake (DPoS) and Proof of Authority (PoA), will make blockchain more sustainable and suitable for industrial-scale deployments. In the IoT domain, blockchain will enable autonomous device-to-device communication and trustless data marketplaces, where devices can exchange verified information and services without intermediaries. Integration with edge computing will further enhance latency-sensitive applications, allowing faster and more secure decision-making at the network periphery. From a policy perspective, the establishment of global standards for blockchain-based security protocols and regulatory frameworks will be crucial to achieving interoperability and compliance. Collaboration among academia, industry, and governments will drive innovation and ensure that blockchain technologies evolve in alignment with ethical, privacy, and societal requirements. Ultimately, the convergence of blockchain, AI, and next-generation networking (such as 6G and quantum internet) will redefine the landscape of cybersecurity—creating systems that are not only reactive but also predictive, self-healing, and transparent.

## 8. Conclusion

Blockchain technology introduces a transformative approach to strengthening network security by replacing centralized trust with distributed consensus and immutable records. Its ability to ensure transparency, data integrity, and resilience has made it an effective tool for mitigating DDoS attacks, facilitating decentralized threat intelligence sharing, and protecting IoT data. The technology's decentralized nature ensures that no single entity can manipulate or compromise the system, thus enhancing the reliability of security operations. From a strategic perspective, blockchain is not merely a technical tool but represents a paradigm shift in cybersecurity architecture, offering a trustworthy platform for both research initiatives and real-world deployments across critical infrastructure sectors. However, blockchain is not a panacea. Challenges such as scalability, energy efficiency, interoperability, and regulatory uncertainty must be addressed for widespread adoption. Continuous advancements in consensus algorithms, cross-chain communication, and integration with AI will be key to realizing blockchain's full potential in cybersecurity. In conclusion, the fusion of blockchain with emerging technologies provides a promising pathway toward a more secure, transparent, and cooperative digital ecosystem. As organizations and researchers continue to explore this integration with the support of conductive policies and cross-sector partnerships, blockchain is poised to evolve into a foundational component of future network security architectures.

## References

[1] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2020). A survey on security and privacy issues of blockchain technology. IEEE Communications Surveys & Tutorials, 22(2), 1191–1219.

[2] Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019). Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 6(2), 2188–2204.

[3] Kumar, K., & Khari, M. (2025). Federated active meta-learning with blockchain for zero-day attack detection in industrial IoT. Peer-to-Peer Networking and Applications.

[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[5] Ram Sundar, G., Rajput, K., Dhanasekaran, S., Aeri, M., Shukla, R. P., & Singh, S. K. (2024). Enhancing network security in distributed environments using blockchain-based solutions. In Proceedings of the International Conference on Data Science and Intelligent Systems (ICDSIS).

[6] Chaganti, R., Bhushan, B., & Ravi, V. (2022). The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions. ArXiv, abs/2202.03617.

[7] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17) (pp. 1093–1110). USENIX Association.

[8] Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. Sensors (Basel, Switzerland), 22(3), 1094.

[9] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. IEEE Access, 9, 57792–57807.

[10] A. Singh et al., 'DDoS attacks and blockchain-based mitigation techniques,' IEEE Access, 2021.

[11] Chatziamanetoglou, D., & Rantos, K. (2021). CTI blockchain-based sharing using proof-of-quality consensus algorithm. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 331–336). IEEE.

[12] Xuan, S., Tang, H., Wang, W., & Yang, W. (2020). Application of blockchain technology in constructing network threat intelligence system. In Proceedings of the 2020 2nd International Conference on Blockchain Technology (ICBCT '20) (pp. 144–149). Association for Computing Machinery.

[13] Shitharth, S., Manoharan, H., Shankar, A., Alsowail, R. A., Pandiaraj, S., Edalatpanah, S. A., & Viriyasitavat, W. (2023). Federated learning optimization: A computational blockchain process with offloading analysis to enhance security. Egyptian Informatics Journal, 24(4), Article 100406.

[14] Kumar, V. N., Veerender, A., Madhukar, G., Soujanya, K. L. S., Naryana, V. A., & Vivekananda, A. (2025). A novel IoT-based blockchain approach for evaluating confidential data sharing by providing data privacy, integrity, and reliability. In V. K. Gunjan, A. Kumar, J. M. Zurada, & S. N. Singh (Eds.), Computational intelligence in machine learning (ICCIML 2023) (Lecture Notes in Electrical Engineering, Vol. 1400). Springer.