Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20250403039
Volume 4, Issue3 (September-December 2025), PP: 249-252.
www.indjcst.com
ISSN No: 2583-5300

Blockchain enabled Cybersecurity: Concepts, Applications and Future Directions

Priyanka Jaiswal[1], Surjeet Kumar Yadav[2]
[1,2] Department of Computer Application, Veer Bahadur Singh Purvanchal University, Jaunpur, Uttar Pradesh, India.

To Cite this Article: *Priyanka Jaiswal[1], Surjeet Kumar Yadav[2], "Blockchain enabled Cybersecurity: Concepts, Applications and Future Directions", Indian Journal of Computer Science and Technology, Volume 04, Issue 03 (September-December 2025), PP: 249-252.*

Abstract: *The continuous growth of interconnected systems, cloud services, and Internet-of-Things (IoT) devices has expanded the attack surface and intensified modern cyber risks, revealing significant weaknesses in centralized security architectures. Blockchain technology, characterized by decentralized control, immutable record-keeping, and cryptographic verification, offers a robust alternative for strengthening cybersecurity across multiple operational domains. This review analyzes the core technical components of blockchain such as distributed ledgers, consensus mechanisms, and network models and explains their relevance to enhancing security functions. It further examines practical applications in network protection, identity and access management, IoT device security, cloud data governance, and software supply-chain assurance. It highlights emerging research directions, including lightweight blockchain solutions for constrained IoT environments, cross-chain security architectures, artificial intelligence-based blockchain threat analytics, and quantum-resilient cryptographic infrastructures.*

Key Words: *Blockchain, Cybersecurity, Decentralized identity, cryptographic hashing etc.*

I. INTRODUCTION

The expansion of digital services, cloud platforms, and Internet-of-Things (IoT) deployments has produced a dramatic growth of cyber threats. Recent analyses show ransomware continues to escalate in frequency and impact, often combining data encryption with exfiltration to enable double-extortion tactics that disrupt healthcare, finance, and public services [1]. Concurrently, the proliferation of connected devices and distributed systems has increased exposure to data breaches, credential theft, and targeted attacks that exploit weak device authentication or inadequate logging [2], [3]. These changing threat dynamics expose limitations in traditional, centrally managed cybersecurity models. The single points of control create single points of failure, centralized logs and authorities provide attractive targets for attackers, and centralized trust assumptions complicate secure coordination across multiple administrative domains and heterogeneous devices.

In response, decentralized architectures based on distributed ledger technologies (DLT), commonly referred to as blockchain, have been proposed as complementary security building blocks. Blockchain's core properties includes an append-only distributed ledger, cryptographic chaining of records, and consensus protocols. This enable tamper-evident audit trails and collective verification without reliance on a single trusted intermediary [4], [5]. These properties can improve data integrity guarantees, support non-repudiable logging, and enable new models of decentralized identity and access control that reduce dependence on centralized credential stores. For example, blockchain approaches have been explored to provide auditable provenance for sensitive healthcare records and to enforce decentralized access policies using smart contracts [4].

Beyond immutable logging and provenance, block-chain can facilitate machine-to-machine trust in IoT ecosystems through lightweight identity anchors and distributed key management, addressing some shortcomings of conventional intrusion detection and authentication schemes in resource-constrained devices [2], [5]. Decentralized architectures also open avenues for secure data marketplaces and privacy-preserving data sharing, where users retain control over consent and access decisions without a single custodian [6]. However, blockchain is not a panacea. Practical challenges such as throughput and latency constraints, consensus costs, privacy leakage through on-chain metadata, and vulnerabilities in smart contracts or integration layers introduce new risk vectors that must be carefully managed [5], [6].

This review aims to synthesize contemporary evidence on where blockchain can realistically strengthen cybersecurity posture and where its limitations constrain adoption. This review aims to guide researchers and practitioners toward realistic, evidence-based uses of blockchain in cybersecurity.

II. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed ledger system in which records are stored across multiple nodes, ensuring data availability, integrity, and resistance to unilateral tampering. Each block contains timestamped transactions linked through cryptographic hashing, forming an immutable chain of records [7]. Merkle trees further enable efficient verification of large transaction sets, while consensus rules determine how participants validate and append new blocks [8].

Blockchains can be categorized into public, private, consortium, and hybrid networks, each exhibiting distinct governance

and security characteristics. Public blockchains maximize transparency and decentralization but expose larger attack surfaces, whereas private and consortium blockchains offer controlled participation with improved performance but reduced trust decentralization [9].

Consensus mechanisms play a central role in blockchain security. Proof of Work (PoW) provides Sybil resistance through computational difficulty [7], while Proof of Stake (PoS) and Delegated PoS improve energy efficiency by assigning block creation rights based on stake ownership [10]. Practical Byzantine Fault Tolerance (PBFT) offers low-latency consensus suitable for permissioned environments, tolerating up to one-third malicious nodes [11]. Proof of Authority (PoA) relies on vetted validators, trading decentralization for operational efficiency. These mechanisms collectively influence blockchain resilience against attacks such as Sybil, double spending, and consensus manipulation.

Blockchain provides a decentralized security architecture capable of addressing several systemic cybersecurity challenges across distributed digital ecosystems. Its immutability and cryptographic chaining of blocks ensure strong data integrity and tamper resistance, preventing unauthorized modification of stored records. Because each transaction is hashed and linked to previous blocks, altering historical data becomes computationally infeasible, making blockchain a reliable integrity-preserving mechanism for logs, medical records, and critical infrastructure telemetry [12].

In authentication and identity management, blockchain supports decentralized identity (DID) systems that eliminate reliance on central authorities. Smart contracts and distributed identifiers allow users to maintain cryptographic control over their credentials, reducing identity theft and credential compromise risks [13]. These mechanisms also enable secure device authentication in IoT ecosystems, where traditional centralized identity frameworks are difficult to scale [14].

For secure data sharing and storage, blockchain provides tamper-proof audit trails and controlled access through smart contracts. Sensitive data can be stored off-chain while blockchain maintains immutable permissions and access logs, enhancing confidentiality and accountability in multi-organization environments.

Blockchain's decentralized design inherently counteracts single points of failure. Since data are replicated across multiple nodes, attacks on a single server do not compromise system availability or integrity, improving resilience against DDoS and data corruption attacks [7]. Regarding insider threat mitigation, blockchain's transparent yet tamper-evident logging restricts unauthorized internal modifications and ensures full traceability of administrative actions, which is crucial in high-risk sectors such as healthcare and finance [13].

The blockchain significantly enhances trust in multi-party systems. Its consensus-driven verification enables mutually distrusting entities to share data and execute transactions without relying on intermediaries, reducing disputes and fostering secure collaboration in supply chains, cloud ecosystems, and federated learning platforms [14].

III. BLOCKCHAIN TECHNOLOGY IN CYBER SECURITY

Blockchain technology has emerged as a foundational security mechanism across multiple cybersecurity domains due to its decentralization, immutability, and transparent auditability. In network security, blockchain enhances resilience against Distributed Denial of Service (DDoS) attacks by decentralizing DNS, distributing traffic, and mitigating single points of failure. By leveraging distributed consensus, blockchain-based systems can validate legitimate routing information and prevent route spoofing, thereby supporting secure routing in large-scale networks. Additionally, the integrity of on-chain logs allows machine learning systems to leverage verified traffic histories, enabling more reliable anomaly detection for identifying malicious flows and coordinated botnet activity [12].

In the domain of Identity and Access Management (IAM), blockchain supports Decentralized Identity (DID) frameworks in which users control cryptographic credentials without dependence on centralized authorities. DID models enhance privacy, reduce credential theft, and provide verifiable authentication suitable for cross-organization applications. Blockchain can also reinforce zero-trust security architectures, where no entity is implicitly trusted, by offering tamper-proof identity verification, policy enforcement via smart contracts, and traceable access decisions, thereby reducing lateral movement risk in enterprise networks [6].

Blockchain's role in IoT security is particularly notable. Resource-constrained IoT devices often lack robust security features, making them vulnerable to spoofing, unauthorized firmware changes, and botnet recruitment. Blockchain enables decentralized device authentication, ensuring that only verified nodes join the network, while smart-contract-based workflows automate secure firmware updates, improving resilience against malicious modification. Lightweight blockchain frameworks such as DAG-based or permissioned blockchains help overcome IoT limitations by reducing computational overhead and latency, making them suitable for edge environments [5].

In cloud security, blockchain enhances confidentiality and integrity through decentralized secure storage models where data provenance, version history, and access rights are immutably recorded. Sensitive data may remain off-chain while metadata, permissions, and integrity hashes are stored on-chain, enabling tamper-evident verification [13]. Similarly, blockchain provides auditable access trails, ensuring transparency in multi-tenant cloud environments by recording administrative actions and access events, thereby improving accountability and compliance monitoring.

Finally, blockchain is increasingly applied in supply chain and software security. The immutability of blockchain enables fine-grained traceability of software components, forming the foundation of blockchain-backed Software Bills of Materials (SBOMs) that document dependencies, versions, and integrity proofs across development pipelines [Saberi]. This transparency helps detect tampered libraries, compromised build systems, and unauthorized insertions in the software lifecycle. Moreover, blockchain's decentralized verification of transactions reduces opportunities for supply-chain attacks, allowing vendors, auditors, and customers to validate provenance without relying on a single trusted intermediary [14].

Across these domains, blockchain strengthens cybersecurity by reducing trust dependencies, improving detection and response capabilities, and enabling verifiable data integrity. While challenges remain related to scalability and integration, blockchain continues to demonstrate significant potential as a complementary security technology.

IV.FUTUTRE DIRECTION

Rosuvastatin 20 mg on every other regimen had equal effect when compared to daily dose regimen of atorvastatin 40 mg &rosuvastatin 20mg. Future research in blockchain-enhanced cybersecurity is increasingly focused on improving scalability, interoperability, intelligence-driven security, and resilience against emerging quantum threats. Lightweight blockchain solutions for IoT aim to address the computational and storage constraints of sensor nodes and embedded devices. Approaches such as DAG-based ledgers, sharded blockchains, and off-chain computation reduce resource overhead while maintaining integrity and authentication guarantees. Studies have demonstrated that lightweight consensus mechanisms, including Proof-of-Authority and optimized PBFT variants, can support decentralized IoT trust without excessive energy consumption [15].

Another critical direction is the development of interoperable security frameworks that enable seamless communication across heterogeneous blockchain networks. As organizations increasingly deploy multiple permissioned and public blockchains, secure cross-chain protocols and standardized identity models are required to enable trust sharing and unified policy enforcement. Emerging interoperability solutions, such as blockchain gateways and cryptographic relays, aim to provide secure data exchange and coordinated cybersecurity operations across disparate ledgers [16].

Advances in AI-driven blockchain threat detection are transforming how anomalies, fraud, and malicious consensus activities are identified. Machine learning models applied to on-chain behavioural data, transaction graphs, and smart-contract execution patterns enable proactive threat prediction and automated forensics. Recent research has explored the use of graph neural networks (GNNs) and federated learning to detect blockchain fraud and Sybil patterns without compromising data privacy [17].

The quantum-safe blockchain architectures represent a long-term priority as quantum computing threatens classical cryptographic primitives such as ECDSA and RSA. Post-quantum signature schemes—lattice-based, hash-based, and multivariate cryptography—are being evaluated for integration into blockchain protocols to ensure long-term immutability and secure transaction verification. Several studies have proposed transitioning blockchains to quantum-resistant key infrastructures and hybrid cryptographic layers to mitigate future quantum adversaries [18].

V.CONCLUSION

Blockchain technology presents a compelling paradigm for enhancing cybersecurity across modern digital infrastructures. Its decentralized architecture, cryptographic integrity, and tamper-resistant ledger provide strong foundations for addressing persistent challenges such as data manipulation, unauthorized access, insecure device onboarding, and opaque supply-chain operations. Through applications in network protection, identity and access management, IoT security, cloud governance, and software traceability, blockchain demonstrates clear potential to reinforce trust, transparency, and resilience in distributed systems. However, the technology is not without limitations. Scalability constraints, privacy concerns, high computational overhead, and the difficulty of integrating blockchain with legacy platforms continue to hinder widespread deployment. These issues underscore the need for ongoing research focused on designing lightweight protocols for resource-constrained environments, developing interoperable and standards-driven security frameworks, and advancing AI-enabled threat detection mechanisms capable of analyzing on-chain behavior. Furthermore, the looming threat of quantum computing necessitates early adoption of quantum-safe cryptographic primitives to ensure long-term robustness of blockchain-based security solutions. Overall, while challenges remain, the synthesis of current research indicates that blockchain is well positioned to become a foundational technology for future cyber defense strategies. Its continued evolution will play a central role in shaping secure, transparent, and trustworthy digital ecosystems.

REFERENCES

[1]. European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape for Ransomware Attacks, Jul. 2022.
[2]. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
[3]. B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” Journal of Network and Computer Applications, vol. 84, pp. 25–37, Apr. 2017.
[4]. M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in Proc. 2016 IEEE 18th Int. Conf. on e-Health Networking, Applications and Services (HealthCom), Munich, Germany, Sep. 2016, pp. 1–3.
[5]. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[6]. E. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in 2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, May 2015, pp. 180–184.
[7]. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. (Foundational technical report; universally cited in SCI/IEEE blockchain research.)
[8]. G. Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger, Ethereum Yellow Paper, 2014.
[9]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” Proc. 2017 IEEE Int. Congr. Big Data, pp. 557–564, 2017.
[10]. S. King and S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” 2012.
[11]. M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” OSDI ’99: USENIX Symposium on Operating Systems Design and Implementation, pp. 173–186, 1999.
[12]. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,” IEEE Access, vol. 7, pp. 164–174, 2019.
[13]. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, “Blockstack: A Global Naming and Storage System Secured by Blockchains,” USENIX ATC, 2016.

[14]. S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain Technology and Its Relationships to Sustainable Supply Chain Management," International Journal of Production Research, vol. 57, no. 7, pp. 2117–2135, 2019.
[15]. T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," IEEE Access, vol. 7, pp. 45201–45218, 2019.
[16]. A. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," ACM Computing Surveys, vol. 54, no. 8, pp. 1–41, 2021.
[17]. J. Wu, J. Liu, Y. Zhang, and K. K. R. Choo, "Fraud Detection in Blockchain Networks: A Graph-Based Machine Learning Approach," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1139–1151, 2021.
[18]. D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," Ledger, vol. 3, pp. 1–21, 2018.