OPEN ACCESS

CITE PUBLICATIONS

Journal of Analytical and Applied Computer Sciences
Volume: 1, Issue: 1, 2025 (December), Pages: 21-25
Review Article

Recent Advances in Blockchain Technology - A Survey of Trends, Challenges, and Research Gaps

K Z Krishna Teja*, S. Savitri, B. Bhuvana Harshitha

Department of Computer Science, Kakaraparti Bhavanarayana College,Vijayawada-520001.

***Correspondence**
K Z Krishna Teja
tejakrishna398@gmail.com

Received: 21 August 2025 / Accepted: 28 November 2025 / Published: 31 December 2025

Blockchain technology has evolved significantly since its introduction as the underlying framework for cryptocurrencies. In recent years, it has expanded into a versatile distributed ledger technology supporting decentralized applications across finance, healthcare, supply chains, governance, and the Internet of Things. This review paper presents a comprehensive survey of recent advances in blockchain technology, focusing on architectural developments, consensus mechanisms, scalability solutions, security enhancements, and emerging application domains. The study critically examines current challenges such as performance limitations, energy consumption, interoperability, privacy concerns, and regulatory uncertainties. By analysing recent literature and technological trends, the paper identifies key research gaps and outlines promising directions for future investigation. The findings aim to support researchers and practitioners in understanding the current state of blockchain technology and its trajectory toward large-scale, sustainable adoption.

Keywords: *Blockchain Technology, Distributed Ledger, Consensus Mechanisms, Scalability, Smart Contracts, Web3, Research Gaps*

Introduction

Blockchain technology is a decentralized and tamper-resistant data structure that enables secure and transparent transactions without reliance on a central authority (Nakamoto, 2008). Originally introduced through Bitcoin, blockchain has progressed far beyond its initial role in cryptocurrency systems and is now considered a foundational technology for decentralized digital ecosystems (Swan, 2015). The core features of immutability, transparency, and distributed consensus have attracted attention from both academia and industry. In recent years, the blockchain landscape has undergone rapid transformation with the emergence of smart contracts, permissioned blockchains, and decentralized applications (DApps) Buterin (2014). Platforms such as Ethereum have enabled programmable blockchain environments, facilitating innovation across diverse sectors. Simultaneously, new consensus mechanisms and architectural models have been proposed to address the performance and energy inefficiencies of early blockchain systems (Castro & Liskov, 1999). Despite these advancements, blockchain technology continues to face critical challenges related to scalability, interoperability, privacy, and governance. Moreover, the pace of innovation has created fragmented research efforts, making it difficult to identify coherent trends and unresolved research problems (Christidis & Devetsikiotis, 2016). This review paper surveys recent developments in blockchain technology, analyses key challenges, and identifies open research gaps that must be addressed to enable widespread adoption.

Evolution of Blockchain Technology

First-Generation Blockchains

First-generation blockchains, exemplified by Bitcoin, were primarily designed for peer-to-peer digital currency transactions (Nakamoto, 2008). These systems relied on Proof of Work (PoW) consensus mechanisms to ensure security and decentralization. While effective, PoW-based systems suffer from limited throughput and high energy consumption (Croman et al., 2016).

Second-Generation Blockchains

Second-generation blockchains introduced smart contracts, enabling programmable transactions and decentralized applications (Buterin, 2014). Ethereum is the most prominent example, supporting complex logic execution on-chain. This advancement significantly expanded blockchain's applicability but also introduced new security vulnerabilities and scalability concerns (Atzei et al., 2017).

Third-Generation and Beyond

Recent blockchain platforms focus on improving scalability, interoperability, and sustainability. Concepts such as sharding, layer-2 solutions, and alternative consensus mechanisms characterize this generation (Wood, 2016). These systems aim to overcome the limitations of earlier designs while maintaining decentralization and security.

Recent Trends in Blockchain Technology

Consensus Mechanism Innovations

To reduce energy consumption and improve performance, many blockchains have transitioned from PoW to alternatives such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) variants (Castro & Liskov, 1999; Wang et al., 2019). These mechanisms offer faster confirmation times and lower operational costs but introduce new trade-offs in decentralization and security.

Scalability Solutions

Scalability remains a major focus of recent research. Layer-2 solutions, including state channels and rollups, process transactions off-chain while preserving on-chain security guarantees (Poon & Dryja, 2016). Sharing techniques divide the blockchain network into smaller partitions to enable parallel transaction processing (Kokoris-Kogias et al., 2018).

Smart Contracts and Automation

Smart contracts have evolved to support increasingly complex decentralized applications. Advances in formal verification and secure programming languages aim to reduce vulnerabilities and enhance reliability (Hirai, 2017). However, smart contract bugs continue to cause significant financial losses.

Blockchain Interoperability

Interoperability solutions enable communication and asset transfer across different blockchain networks. Cross-chain bridges and interoperability protocols have emerged as critical components of the blockchain ecosystem (Zamyatin et al., 2021).

Application Domains

Financial Services and DeFi

Decentralized Finance (DeFi) leverages blockchain to provide financial services such as lending, trading, and asset management without intermediaries (Schär, 2021). While DeFi demonstrates blockchain's disruptive potential, it also raises concerns related to security, volatility, and regulation.

Supply Chain Management

Blockchain enhances supply chain transparency and traceability by providing immutable records of product movement and provenance (Kim & Laskowski, 2018). Adoption challenges include integration with legacy systems and data authenticity.

Healthcare Systems

In healthcare, blockchain supports secure data sharing, patient-centric record management, and auditability (Azaria et al., 2016). Privacy preservation and regulatory compliance remain critical issues.

Internet of Things (IoT)

Blockchain-IoT integration enables decentralized device management and secure data exchange. However, resource constraints and latency pose challenges for large-scale deployment (Conoscenti et al., 2016).

Security and Privacy Advances

Recent research has focused on improving blockchain security through cryptographic enhancements, intrusion detection systems, and decentralized identity frameworks (Atzei et al., 2017; Li et al., 2020). Privacy-preserving techniques such as zero-knowledge proofs and confidential transactions allow sensitive data to be protected while maintaining transparency (Sasson et al., 2014). Despite these advances, attacks on smart contracts and cross-chain bridges remain prevalent.

Key Challenges in Blockchain Adoption

Scalability and Performance

Even with recent improvements, many blockchain systems struggle to match the throughput and latency of traditional centralized systems (Croman et al., 2016).

Energy Efficiency and Sustainability

Energy consumption remains a concern, particularly for PoW-based systems. Sustainable blockchain design is an active area of research (Wang et al., 2019).

Interoperability and Standardization

The lack of common standards complicates cross-platform interaction and ecosystem integration Zamyatin et al., 2021.

Legal and Regulatory Issues

Unclear regulatory frameworks and jurisdictional differences hinder enterprise adoption and public trust (Schär, 2021).

Research Gaps and Open Issues

Despite significant progress, several research gaps remain:

- Lack of standardized benchmarking frameworks for performance and security
- Limited empirical evaluation of interoperability solutions
- Insufficient integration of privacy mechanisms with scalable architectures
- Governance models for decentralized systems remain underexplored
- Long-term sustainability of token-based incentive mechanisms addressing these gaps is essential for blockchain’s transition from experimental technology to mainstream infrastructure (hristidis & Devetsikiotis, 2016; Lin & Liao, 2017).

Future Research Directions

Future work should focus on holistic blockchain architectures that balance scalability, security, and decentralization. Greater emphasis on real-world deployment studies, regulatory-aware design, and energy-efficient consensus mechanisms is required. Interdisciplinary research combining blockchain with AI, IoT, and edge computing is expected to shape next-generation decentralized systems.

Conclusion

This review paper has surveyed recent advances in blockchain technology, highlighting key trends, application domains, and persistent challenges. While blockchain has evolved into a versatile and powerful technology, its widespread adoption is constrained by technical, organizational, and regulatory barriers. By identifying current research gaps and future directions, this study provides a foundation for continued innovation and informed development of blockchain-based systems.

Author contributions

K. Z. Krishna Teja conceptualized the study, designed the review framework, and coordinated the overall structure of the manuscript.

S. Savitri conducted the literature survey on consensus mechanisms, scalability solutions, and interoperability, and contributed to drafting the manuscript.

B. Bhuvana Harshitha analyzed application domains, security and privacy advances, research gaps, and future directions, and assisted in manuscript revision.

All authors reviewed, revised, and approved the final version of the manuscript.

Funding

No funding.

Conflict of interest

The authors declare that there is no conflict of interest, financial or non-financial, related to the publication of this article.

Ethics approval

This study is a review-based research work conducted using previously published literature only. It does not involve human participants, animals, or sensitive personal data. Therefore, ethical approval and informed consent are not applicable.

AI tool usage declaration

The authors declare that AI-assisted tools were used solely for language editing, grammar correction, and formatting assistance during manuscript preparation. All technical content, analysis, interpretations, and conclusions were entirely developed and verified by the authors. No AI system was used to generate original research ideas, data, or scientific findings.

References

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

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly.

Buterin, V. (2014). *Ethereum: A next-generation smart contract platform*.

Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In *Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI)*.

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292–2303.

Croman, D., et al. (2016). On scaling decentralized blockchains. In *Financial Cryptography and Data Security (FC)*.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts. In *Financial Cryptography and Data Security (FC)*.

Wood, G. (2016). *Polkadot: Vision for a heterogeneous multi-chain framework*.

Wang, Q., et al. (2019). Blockchain consensus mechanisms: A survey. *IEEE Systems Journal, 13*(3), 1–20. https://doi.org/10.1109/JSYST.2018.2888518

Poon, J., & Dryja, T. (2016). *The Bitcoin Lightning Network: Scalable off-chain instant payments*.

Kokoris-Kogias, E., et al. (2018). OmniLedger: A secure, scale-out, decentralized ledger via sharding. In *IEEE Symposium on Security and Privacy (S&P)*.

Hirai, Y. (2017). Defining the Ethereum virtual machine for interactive theorem provers. In *Financial Cryptography and Data Security (FC)*.

Zamyatin, A., et al. (2021). SoK: Communication across distributed ledgers. In *IEEE Symposium on Security and Privacy (S&P)*.

Schär, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review, 103*(2), 153–174.

Kim, T. H., & Laskowski, J. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. In *International Conference on Blockchain and Cryptocurrency (ICBC)*.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Open & Big Data Conference*.

Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. *IEEE Communications Surveys & Tutorials, 18*(3), 1259–1273.

Li, W., et al. (2020). A survey on blockchain security: Vulnerabilities, attacks, and applications. *Future Generation Computer Systems, 107*, 841–853.

Sasson, E. B., et al. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. In *IEEE Symposium on Security and Privacy (S&P)*.

Lin, I.-C., & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *International Journal of Network Security, 19*(5), 653–659.