International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0322
e ISSN: 2584-2854
Volume: 03
Issue:05 May 2025
Page No: 2059 - 2064

A Review Paper On: Blockchain Technology Behind Cryptography

DR. Pushparani MK[1], Abhishekgouda B D[2], Harsh Umarjikar[3], G Chethan[4], Gowtham G[5]
[1]Associate professor, Dept. of CSD, Alva's Institute of Engg. & Tech., Moodbidri, Karnataka, India.
[2,3,4,5]UG Scholar, Dept. of CSD, Alva's Institute of Engg. & Tech., Moodbidri, Karnataka, India.
Email ID: *drpushparani@aiet.org.in[1], dyavanagoudrabhishek@gmail.com[2], harshumarji644@gmail.com[3], gchethangowda785@gmail.com [4], gowthamggowthu74@gmail.com[5]*

Abstract
Blockchain technology has garnered significant attention primarily through its association with cryptocurrencies like Bitcoin. However, its potential applications extend far beyond digital currencies, offering transformative solutions across diverse industries. This paper reviews the advancements in blockchain technology and explores its use cases in fields such as supply chain management, healthcare, finance, governance, and data security. The decentralized and immutable nature of blockchain enables enhanced transparency, traceability, and efficiency in these domains, addressing long-standing challenges such as fraud, data tampering, and inefficient processes. Emerging trends such as blockchain-based smart contracts, decentralized finance (DeFi), and secure identity management are discussed, showcasing how the technology is reshaping traditional frameworks. By analyzing these developments, this paper highlights the far-reaching implications of blockchain technology and emphasizes its role as a cornerstone of the digital revolution.

Keywords: *Blockchain Technology, Decentralized Systems, Financial Technology (FinTech), Governance and Transparency, Data Security and Privacy, Decentralized Finance (DeFi), Digital Identity Management.*

1. Introduction
Blockchain technology has emerged as a transformative innovation at the heart of the cryptocurrency revolution. Originally conceptualized as the underlying infrastructure for Bitcoin in 2008 by the pseudonymous Satoshi Nakamoto, blockchain has since evolved beyond digital currencies, influencing a wide range of industries including finance, supply chain, healthcare, and governance. At its core, blockchain is a decentralized, distributed ledger that enables secure, transparent, and tamper-resistant recording of transactions without the need for a central authority [1]. This review paper focuses on the technical foundation of blockchain technology as it pertains to cryptocurrencies. It explores the fundamental principles such as decentralization, consensus mechanisms, cryptographic security, and smart contracts that empower blockchain systems. Additionally, it examines the evolution of blockchain architectures (from public to private and consortium models), the challenges of scalability, energy efficiency, and regulatory concerns, and the potential future developments in the space. By analyzing both foundational concepts and recent advancements, this paper aims to provide a comprehensive understanding of how blockchain technology supports the operation and growth of cryptocurrencies, and what it means for the future of digital finance [2][3].

1.1 Literature and Review
Over the past decade, blockchain technology has garnered increasing academic and industrial attention due to its association with cryptocurrencies and its potential to disrupt traditional financial systems. Numerous studies have been conducted to understand and enhance the underlying mechanisms, security features, and performance of blockchain networks. Nakamoto (2008) introduced the first decentralized cryptocurrency, Bitcoin, which utilized a Proof-of-Work (PoW) consensus mechanism to secure transactions on a peer-to-peer network. This seminal

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0322
e ISSN: 2584-2854
Volume: 03
Issue:05 May 2025
Page No: 2059 - 2064

work laid the groundwork for subsequent blockchain-based systems. Since then, researchers have explored alternative consensus protocols such as Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT), aiming to improve scalability, energy efficiency, and transaction throughput (Zheng et al., 2018; Wang et al., 2019). Yli-Huumo et al. (2016) conducted a systematic review of blockchain research, identifying key areas such as scalability, latency, throughput, and data privacy as critical limitations. Their findings highlighted the need for continued development in network performance and smart contract security. Similarly, Li et al. (2020) emphasized the importance of consensus mechanism design and its trade-offs in terms of decentralization, security, and scalability. Recent works have also focused on the evolution of blockchain platforms. Ethereum introduced smart contracts, expanding blockchain's utility beyond currency to programmable decentralized applications (DApps) [4]. Studies by Buterin (2015) and Wood (2014) illustrate how Ethereum enables autonomous code execution on a distributed ledger, though concerns regarding security vulnerabilities (e.g., the DAO hack) remain prevalent in literature. Other researchers have examined blockchain adoption challenges, including regulatory uncertainty, user anonymity, and cross-chain interoperability. Tapscott & Tapscott (2016) emphasized the socio-economic implications of blockchain, while academic discourse continues to explore governance models and sustainable implementations of blockchain for public and private use cases. In summary, existing literature presents a broad and growing body of knowledge addressing the foundational principles, technical challenges, and emerging opportunities associated with blockchain technology in the context of cryptocurrencies. This review paper builds upon these works to synthesize key developments and identify future research directions [5-11].

2. Challenges and Future Directions

Despite its transformative potential, blockchain technology especially in the context of cryptocurrencies faces several significant challenges that hinder its widespread adoption and optimal performance.

2.1 Challenges

Scalability: One of the most pressing issues is scalability. Public blockchains like Bitcoin and Ethereum can handle only a limited number of transactions per second (TPS), far below traditional financial systems like Visa. Solutions such as Layer 2 protocols (e.g., Lightning Network) and sharding are being explored but remain under active development. Energy Consumption: Proof-of-Work (PoW)-based cryptocurrencies consume enormous amounts of energy, raising environmental concerns. Ethereum's shift to Proof-of-Stake (PoS) with its "Merge" upgrade aims to mitigate this, but energy efficiency remains a core concern across many blockchain platforms. Security Vulnerabilities: Smart contracts, once deployed, are immutable and often lack proper auditing, making them vulnerable to bugs and exploitation as seen in the infamous DAO hack. Ensuring robust security frameworks for decentralized applications (DApps) is an ongoing challenge. Regulatory Uncertainty: The decentralized nature of cryptocurrencies poses regulatory dilemmas for governments and financial institutions. Issues like anti-money laundering (AML), know-your-customer (KYC) compliance, and taxation are still being addressed inconsistently across jurisdictions. Interoperability: Many blockchain networks operate in isolation, making it difficult for assets and data to move seamlessly between them. Cross-chain solutions are in development but have yet to become standardized [12-14].

2.2 Future Directions

Enhanced Consensus Mechanisms: Research into alternatives to PoW, such as PoS, DPoS, and hybrid models, continues to be a priority. These mechanisms promise better energy efficiency and faster transaction times. Blockchain Interoperability: Future platforms are likely to prioritize interoperability to enable secure and efficient communication between different blockchains. Projects like Polkadot and Cosmos are pioneering this area. Scalable Layer 2 Solutions: Technologies like rollups, sidechains, and state channels are expected to play a major role in overcoming scalability limitations without compromising decentralization or security. Quantum-Resistant

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0322
e ISSN: 2584-2854
Volume: 03
Issue:05 May 2025
Page No: 2059 - 2064

Cryptography: With the advancement of quantum computing, the cryptographic algorithms underpinning current blockchains may become vulnerable. Research into post-quantum cryptography is critical for future-proofing blockchain systems. Legal and Regulatory Frameworks: The development of global, harmonized regulatory standards could provide greater clarity and trust, encouraging mainstream adoption and institutional investment in cryptocurrencies. Integration with Emerging Technologies: Blockchain is increasingly being integrated with AI, IoT, and edge computing to create smarter, decentralized ecosystems. These synergies may unlock new use cases and business models [15].

3. Consensus Mechanisms

Consensus mechanisms are the backbone of blockchain networks, ensuring that all nodes in a decentralized system agree on the validity of transactions and the state of the ledger. In the absence of a central authority, these protocols maintain security, prevent double-spending, and enable trustless operation.

3.1 Proof of Work (PoW)

PoW is the first and most well-known consensus mechanism, introduced by Bitcoin. It requires network participants (miners) to solve complex cryptographic puzzles to validate transactions and create new blocks. Although highly secure, PoW is criticized for its energy-intensive process and relatively low transaction throughput. Advantages: Strong security, resistance to Sybil attacks. Disadvantages: High energy consumption, limited scalability. Example: Bitcoin, early Ethereum [16].

3.2 Proof of Stake (PoS)

PoS selects validators based on the amount of cryptocurrency they "stake" as collateral. This mechanism significantly reduces energy consumption compared to PoW. Validators are rewarded for confirming blocks and penalized for malicious behavior. Advantages: Energy efficiency, faster transaction finality. Disadvantages: Wealth centralization risk, potential for “nothing at stake” problem. Example: Ethereum 2.0, Cardano.

3.3 Delegated Proof of Stake (DPoS)

DPoS is a variant of PoS where token holders elect a small group of delegates to validate transactions and maintain the blockchain. It enhances scalability and speed but can compromise decentralization. Advantages: High performance, low latency. Disadvantages: Increased centralization risk. Example: EOS, Tron.

3.4 Practical Byzantine Fault Tolerance (PBFT)

PBFT is designed for permissioned blockchains, where nodes are known and trusted. It allows fast and deterministic consensus, even in the presence of malicious actors, but is less scalable due to its communication complexity. Advantages: Low energy usage, high throughput. Disadvantages: Poor scalability in public networks. Example: Hyperledger Fabric, Ripple.

3.5 Hybrid Mechanisms and Emerging Protocols

Modern blockchains often combine multiple consensus mechanisms to balance performance and decentralization. For example, Algorand uses Pure PoS, while Polkadot and Cosmos explore custom hybrid models to address scalability and interoperability. Each consensus mechanism presents trade-offs between security, decentralization, scalability, and energy consumption. The choice of protocol significantly influences the design and functionality of a cryptocurrency, making it a crucial area of ongoing research and innovation [18].

4. Blockchain Platforms for Cryptocurrency

Blockchain platforms serve as the foundational infrastructure for cryptocurrencies, enabling secure, transparent, and decentralized digital transactions. Each platform is designed with unique features, consensus mechanisms, and scalability approaches, tailored to specific use cases within the broader cryptocurrency ecosystem. This section reviews major blockchain platforms that have significantly influenced the development and adoption of cryptocurrencies [17][19].

4.1 Bitcoin

Bitcoin is the first and most widely recognized blockchain-based cryptocurrency, launched in 2009 by the pseudonymous Satoshi Nakamoto. It uses a Proof of Work (PoW) consensus mechanism and is primarily designed as a decentralized peer-to-peer currency. Bitcoin focuses on security and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0322
e ISSN: 2584-2854
Volume: 03
Issue:05 May 2025
Page No: 2059 - 2064

decentralization but suffers from low transaction throughput and high energy consumption. Use Case: Digital store of value and medium of exchange. Limitations: Scalability, energy inefficiency, limited scripting capability.

4.2 Ethereum

Launched in 2015, Ethereum introduced the concept of smart contracts, enabling decentralized applications (DApps) to be built on the blockchain. Initially based on PoW, Ethereum transitioned to Proof of Stake (PoS) with the Merge in 2022 to improve scalability and energy efficiency. It is a leading platform for DeFi, NFTs, and DAO projects. Use Case: Smart contracts, decentralized finance (DeFi), NFTs. Strengths: Programmability, large developer community. Limitations: Congestion, high gas fees.

4.3 Cardano

Cardano is a third-generation blockchain that uses the Ouroboros PoS consensus protocol. Emphasizing a research-driven approach, it aims to solve scalability, sustainability, and interoperability issues. Cardano supports smart contracts and seeks to balance security with performance. Use Case: Secure and scalable smart contract platform. Strengths: Formal verification, low energy usage. Limitations: Slower development due to peer-reviewed model.

4.4 Polkadot

Polkadot focuses on interoperability and scalability through its unique multichain architecture. It connects multiple specialized blockchains (parachains) via a central Relay Chain. Polkadot uses a Nominated Proof of Stake (NPoS) model and is designed to support cross-chain transfers of data and assets. Use Case: Blockchain interoperability, multichain ecosystem. Strengths: Scalability, flexibility. Limitations: Complex architecture, still maturing.

4.5 Solana

Solana is a high-performance blockchain known for its extremely fast transaction speeds and low fees. It combines Proof of Stake with Proof of History (PoH) to achieve high throughput [22]. Solana is well-suited for decentralized applications that require speed, such as gaming and high-frequency trading. Use Case: High-speed DApps, DeFi, NFTs. Strengths: High TPS, low latency. Limitations: Network instability and outages.

5. Results and Discussion

Blockchain technology has evolved significantly since the introduction of Bitcoin. First-generation blockchains like Bitcoin focused on secure, decentralized value transfer, but lacked programmability. Ethereum marked the transition to second-generation blockchains, enabling smart contracts and decentralized applications (DApps). More recent platforms such as Cardano, Polkadot, and Solana aim to address the “blockchain trilemma” by optimizing for scalability, security, and decentralization simultaneously. Consensus Mechanism Trade-offs: Different consensus mechanisms offer distinct advantages and limitations. PoW, while highly secure, is energy-intensive and slow. PoS and its variants improve efficiency and scalability, but may introduce new risks, such. Future Outlook: The future of blockchain in cryptocurrency appears promising, with increased focus on eco-friendly consensus models, interoperability frameworks, and integration with AI and IoT systems. A shift toward regulatory clarity and improved user experience could further accelerate mainstream adoption and innovation [20].

Conclusion

In conclusion, this Blockchain technology has revolutionized the way digital assets are created, managed, and transferred, with cryptocurrencies being its most prominent and transformative application. This review has explored the foundational principles of blockchain, including decentralization, consensus mechanisms, and cryptographic security, while also examining the strengths and limitations of major blockchain platforms like Bitcoin, Ethereum, Cardano, Polkadot, and Solana [21]. The analysis reveals that while blockchain offers unparalleled security, transparency, and decentralization, it still faces critical challenges such as scalability, energy consumption, regulatory uncertainty, and interoperability. The evolution from energy-intensive Proof of Work systems to more sustainable and scalable models like Proof of Stake and hybrid consensus protocols marks a significant step forward

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0322
e ISSN: 2584-2854
Volume: 03
Issue:05 May 2025
Page No: 2059 - 2064

in addressing these concerns. Looking ahead, the continued development of Layer (2) solutions, cross-chain interoperability, and quantum-resistant cryptography, along with clearer global regulations, will be crucial to the broader adoption of blockchain-based cryptocurrencies [23]. As innovation progresses, blockchain is poised to play a foundational role in the future of finance, governance, and decentralized digital ecosystem.

References

Journal reference style

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

[2]. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853.

[3]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. 2017 IEEE International Congress on Big Data (BigData Congress), 557–564.

[4]. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), 218.

[5]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81.

[6]. Zangana, H. M., & Omar, M. (2020). Threats, Attacks, and Mitigations of Smartphone Security. Academic Journal of Nawroz University, 9(4), 324-332.

[7]. Zangana, H. M., Tawfiq, N. E., & Omar, M. (2020). Advantages and Challenges of E-Government in Turkey.

[8]. Zhang, H., Wu, J., Pan, Q., Bashir, A. K., & Omar, M. (2024). Toward Byzantine-Robust Distributed Learning for Sentiment Classification on Social Media Platform. IEEE Transactions on Computational Social Systems. IEEE.

[9]. Zhou, S., Ali, A., Al-Fuqaha, A., Omar, M., & Feng, L. (n.d.). Robust Risk-Sensitive Task Offloading for Edge-Enabled Industrial Internet of Things. IEEE Transactions on Consumer Electronics.

[10]. Fawzi, D., & Omar, M. (n.d.). New insights to database security: An effective and integrated approach to applying access control mechanisms and cryptographic concepts in Microsoft access environments. Academic Press.

[11]. Gholami, S. (2024). Can pruning make large language models more efficient? In Redefining Security With Cyber AI (pp. 1-14). IGI Global.

[12]. Gholami, S. (2024). Do Generative large language models need billions of parameters? In Redefining Security With Cyber AI (pp. 37-55). IGI Global.

[13]. Gholami, S., & Omar, M. (2023). Does Synthetic Data Make Large Language Models More Efficient? arXiv preprint arXiv:2310.07830.

[14]. Gholami, S., & Omar, M. (2024). Can a student large language model perform as well as its teacher? In Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology (pp. 122-139). IGI Global.

[15]. Hamza, Y. A., & Omar, M. D. (2013). Cloud computing security: abuse and nefarious use of cloud computing.

[16]. International Journal of Computer Engineering Research, 3(6), 22-27.

[17]. Huff, A. J., Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Burton, S. L., Jones, A. J., Springs, D., Omar

[18]. Abbasi, R., Bashir, A. K., Mateen, A., Amin, F., Ge, Y., & Omar, M. (2023). Efficient Security and Privacy of Lossless Secure Communication for Sensor-based Urban Cities. IEEE Sensors Journal. IEEE.

[19]. Ahmed, A., Rasheed, H., Bashir, A. K., & Omar, M. (2023). Millimeter-wave channel modeling in a VANETs using coding techniques. PeerJ Computer Science, 9, e1374. PeerJ Inc.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0322
e ISSN: 2584-2854
Volume: 03
Issue:05 May 2025
Page No: 2059 - 2064

[20]. Information. International Journal Of Computer Sciences And Engineering, 8, 8-12.
[21]. Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smartphones. Journal of Information Systems Technology and Planning, 5(14), 40-60.
[22]. Xu, X., Wu, J., Bashir, A. K., & Omar, M. (2024). Machine Learning and Zero Knowledge Empowered Trustworthy Bitcoin Mixing for Next-G Consumer Electronics Payment. IEEE Transactions on Consumer Electronics. IEEE.
[23]. Zangana, H. M. (2015). A New Skin Color Based Face Detection Algorithm by Combining Three Color Model Algorithms. IOSR J. Comput. Eng, 17, 06-125.