

Security in Blockchain - A Review of Mechanism, Use Cases, Challenges, and Future Directions

Prachi chaniyara¹, Mr. Amrish Patel²

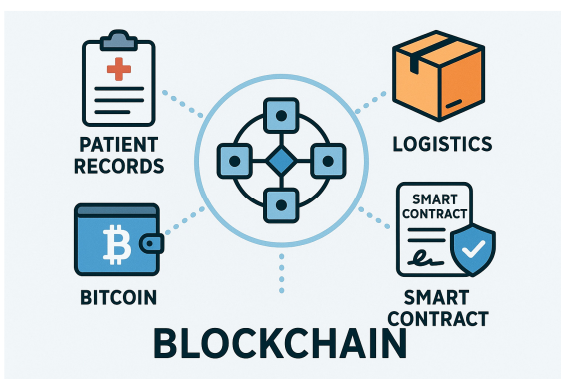
¹(B Tech in Computer Engineering, Atmiya University, Rajkot, India
Email: prachichaniyara@gmail.com)

²(Faculty of Engineering and Technology (CE), Atmiya University, Rajkot, India
Email: amrish.patel@atmiyauni.ac.in)

Abstract-Blockchain has been tested in supply chains, healthcare, and finance and promises transparent, tamper-resistant records. However, the technology also raises new security issues: cross-chain links pose new risks, endpoints and smart contracts are regularly attacked, and industry and regional legal and regulatory requirements vary. This paper identifies lingering issues and potential solutions (post-quantum cryptography, artificial intelligence-powered evaluation, and independent identity), illustrates practical use fields (healthcare and port supply chain), and describes the core elements of security (consensus and cryptography). The key conclusion is that, while blockchain can boost trust in certain contexts, its practical security necessitates layered defenses, meticulous engineering, and regulatory alignment.

I. Introduction

For systems that require trusted records without centralized authority, blockchain's fundamental concept—a distributed ledger that multiple parties share and cannot silently alter—makes it instantly appealing. Issues like damaged records for patients in the medical field or fake goods in logistics can be resolved with the help of this feature.



However, the decentralization that makes blockchain so powerful also changes how vulnerable systems are. These days, attacks

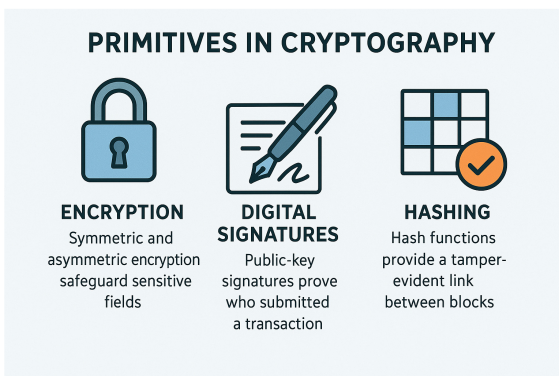
concentrate on more than just the exact locations and techniques of system weaknesses. Bitcoin wallets, smart contracts, and the bridges that link different blockchains are now the targets of attacks instead of just central servers. Real-world implementations must therefore see blockchain as part of a more complex system, where consensus and cryptography provide the framework and design, key management, and governance determine practical security

II. Fundamental components of security

Primitives in cryptography

Blockchain security is fundamentally based on encryption, digital signatures, and hashing. Public-key signatures prove who submitted a transaction; symmetric and asymmetric encryption safeguard sensitive fields; hash functions provide a tamper-evident link between blocks. National cryptographic suites, such as the SM family used in China, are used in some recent applied work to

support differentiated encryption strategies, encrypting highly sensitive fields more robustly than benign metadata. The lesson is to select the appropriate crypto based on the legal environment and the sensitivity of the data.



Confidence and supply agreement

Although robust, Proof-of-Work is costly. Although it uses less energy, Proof-of-Stake exposes more areas for attack. For speed and finality, permissioned systems frequently favor consensus methods like PBFT. Notary or oracle-based cross-chain schemes can simplify ecosystems that span multiple blockchains, but they also add trusted middlemen that need to be secured. Since private, inter-organizational ledgers and public, permissionless networks have different requirements, the consensus model should be appropriate for the use case.

III. Selected security patterns and application domains

Port logistics and the supply chain

Blockchain-based digitization of shipment records and warehouse receipts lowers paper fraud and enhances traceability. While a management layer organizes sharing, multi-chain architectures can isolate specific data from those who require it. Common implementations use layered data

models and limited encryption to guarantee that only authorized parties can read sensitive fields. The ledger could become a single location where many transactions are exposed by compromised keys if key management and access controls are not implemented properly.

Ecosystems of healthcare and medical devices

Healthcare facilities hold some of the most private information. Although blockchain can provide unchangeable audit trails and support patient consent models, related medical equipment and the supply chain for medical goods carry additional risks. Risk assessment frameworks that combine AI-assisted monitoring and blockchain audit logs facilitate anomaly detection and speed up incident response. However, any design needs to start with regulatory compliance (like GDPR or medical device standards).

IV. Practical vulnerabilities and recurring failures

Interfaces and digital wallets. Most malicious attempts exploit weakly secured endpoints, like user wallets and trading APIs, rather than cryptographic primitives.

Smart contract bugs. Contract code errors that have been repeatedly exploited include reentry, integer overflows, and unauthorized entry controls. Risk is reduced by rigorous testing and formal verification.

Chain-spanning bridges. Attackers target bridges that move assets between chains, and breaches of these crossings have led to many significant losses.

Key management. Single points of failure, inadequate storage, or inadequate key rotation

often lead to catastrophic compromise in KMS/HSM configurations.

Regulations are not aligned. Regionally specific security and safety requirements complicate multinational deployments.

V. Future research and directional solutions

post-quantum preparedness. Many well-known elliptic-curve schemes will become vulnerable as quantum computing develops. For systems with long-lived data, the evaluation and transition to quantum-resistant algorithms should begin immediately. security with the aid of AI. Machine learning can be used to identify subtle anomalies in transaction patterns or device behavior. When AI is incorporated into tracking and incident response, defenders can identify and address problems faster; however, the AI models one another must be safeguarded against threats such as prompt injection and model poisoning.

Decentralized identification and private information. By allowing users want to publish their data without any permissions, verified identities and DID systems it improve security in global world as healthcare.

Selective disclosure and decentralised identity. In international use cases such as healthcare, DID systems and authentic credentials improves their privacy with the use of allowing users to show their attributes without releasing their entire data

VI. Conclusion

Although the notion that "blockchain is equal to trustworthy is over simplified, blockchain provides practical tools for creating more reliable systems. The technology removes reliance on a single custodian by fusing digital consensus

protocols, and management processes. Proper cryptography, a strong consensus selected for the use case, hardened endpoints, formal smart contract verification, resilient key management, and regulatory compliance are all essential components of real security. Combining post-quantum crypto, AI-backed monitoring, and secure identity systems is the best way to safely realize the blockchain's potential in the future.

VII. References

- [1] 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.
- [2] Yakubu, M. M., Hassan, F. B., Danyaro, K. U., Junejo, A. Z., Siraj, M., Yahaya, S., ... & Abdulsalam, K. (2024). A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges. *Computer Systems Science & Engineering*, 48(6).
- [3] Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed iot network. *Ieee Access*, 9, 13938-13959.
- [4] Le, T. V., & Hsu, C. L. (2021). A systematic literature review of blockchain technology: Security properties, applications and challenges. *Journal of Internet Technology*, 22(4), 789-802.
- [5] Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S., & Embong, A. H. (2021, August). A review on blockchain security issues and challenges. In *2021 IEEE 12th control and system graduate research colloquium (ICSGRC)* (pp. 227-232). IEEE.

[6] Khamar, J., & Patel, H. (2021). An Extensive Survey on Consensus Mechanisms for Blockchain Technology. In *Data Science and Intelligent Applications*. Springer.

[7] Lin, I. C., & Liao, T. C. (n.d.). *A Survey of Blockchain Security Issues and Challenges*.

[8] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

[9] Karame, G. O. (n.d.). *On the Security and Scalability of Bitcoin's Blockchain*.

[10] Virmani, C., Gupta, D., & Choudhary, T. (n.d.). *Blockchain 2.0*.

[11] Wang, X., & Wu, L. (n.d.). *Operations Research in the Blockchain Technology*.

[12] Lee, J. H. (2019). *Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems*.

[13] Bhutta, M. N. M., Khwaja, A. A., et al. (2021). *A Survey on Blockchain Technology: Evolution, Architecture and Security*. IEEE Access.