International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 7, Issue 1, 260-265, 2026
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V7I1P144

Original Article

Blockchain Technology Explained: A Comprehensive Overview

Shimul Shah
Independent Researcher, Philadelphia, United States.

Received On: 25/01/2026 Revised On: 26/02/2026 Accepted On: 28/02/2026 Published on: 01/03/2026

Abstract - *Traditional network security mechanisms, such as firewalls, intrusion detection systems, and cryptographic protocols, are increasingly inadequate against sophisticated cyberattacks in modern distributed environments. As architectures like the Internet of Things (IoT) and cloud computing expand, ensuring data integrity, privacy, and trustworthy management becomes more complex. In this context, blockchain technology offers a promising paradigm for strengthening network security through decentralization, immutability, and cryptographic consensus. This paper explores blockchain's role in bolstering data security, emphasizing integrity, transparency, and immutability within digital systems. It reviews real-world uses in secure data sharing and identity management, demonstrating how these address modern threats, while employing a qualitative approach to assess existing solutions—their strengths alongside drawbacks like technological immaturity, high costs, complexity, and regulatory obstacles. Ultimately, it posits that effective deployment hinges on tailoring to organizational contexts, defining precise goals, and overcoming these challenges. This study offers a thorough examination of blockchain technology, covering its evolution, structure, core mechanics, constraints, and diverse applications. It delves into foundational traits like decentralization, immutability, and transparency, alongside key concepts, use cases, and ongoing issues, wrapping up with an evaluation of its current landscape, promising horizons, and primary barriers to broad uptake.*

Keywords - *Blockchain, Distributed Ledger, Cybersecurity, Network Security, Decentralized Identity, Secure Network Management, Cryptocurrency.*

1. Introduction

Computer systems and the internet have transformed the ways in which data is stored, transmitted, and accessed, making robust data protection a central concern for contemporary organizations. As cyber-attacks grow increasingly complex and sophisticated, existing defense mechanisms often prove insufficient, since adversaries continually develop new techniques to circumvent established security controls. This dynamic threat landscape underscores the need for continuous research and innovation to enhance and adapt security architectures. In this context, blockchain technology has emerged as a promising foundation for secure, decentralized data and transaction management, extending far beyond its initial association with cryptocurrencies such as Bitcoin. Conceptualized as a decentralized, distributed, and immutable digital ledger, blockchain records transactions across a network of nodes in a transparent, tamper-resistant, and verifiable manner without reliance on a central authority. By organizing transactions into cryptographically linked blocks, it provides an ordered and tamper-evident record of events, which has made it attractive for applications ranging from digital currencies and supply chain management to digital identity, healthcare, voting, and cybersecurity. At the same time, open challenges related to scalability, energy efficiency, interoperability, privacy, and regulatory and usability concerns continue to motivate intensive research efforts. Against this backdrop, the present paper explores the principles, architecture, and operational mechanisms of blockchain technology and critically assesses its strengths, limitations, and emerging applications, with a particular focus on its potential to enhance data security and trust in distributed environments.

1.1. Block Chain Architecture – How it works

Blockchain architecture underpins decentralized ledger systems by structuring data into tamper-resistant blocks linked across distributed networks, guaranteeing immutability, transparency, and security via cryptographic hashing and consensus mechanisms.

1.2. Core Components of Blockchain

- Node: Nodes are network participants and their devices permit them to keep track of the distributed ledger and serve as communication hubs in various network tasks. A block broadcasts all the network nodes when a miner looks to add a new block in transactions to the blockchain.
- Transactions: A transaction refers to a contract or agreement and transfers of assets between parties. The asset is typically cash or property. The network of computers in blockchain stores the transactional data as a copy with the storage typically referred to as a digital ledger.
- Block: A block in a blockchain network is similar to a link in a chain. In the field of cryptocurrency,

blocks are like records that store transactions like a record book, and those are encrypted into a hash tree. There are a huge number of transactions occurring every day in the world. The users need to keep track of those transactions, and they do it with the help of a block structure. The block structure of the blockchain is mentioned in the very first diagram in this article.

- Chain: Chain is the concept where all the blocks are connected with the help of a chain in the whole blockchain structure in the world. And those blocks are connected with the help of the previous block hash and it indicates a chaining structure.
- Miners: Blockchain mining is a process that validates every step in the transactions while operating all cryptocurrencies. People involved in this mining they called miners. Blockchain mining is a process to validate each step in the transactions while operating cryptocurrencies.

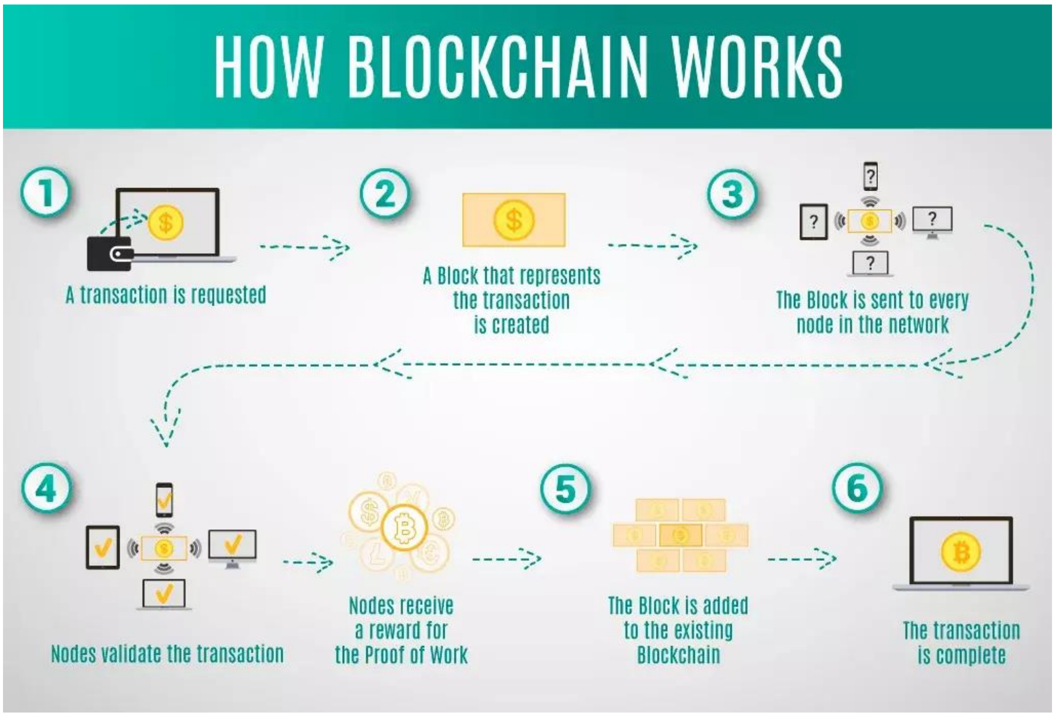
HOW BLOCKCHAIN WORKS
1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Fig 1: How Blockchain works. Adapted from by Anastasiia Lastovetska – November 12, 2021

Source: *https://mlsdev.com/blog/156*

- Consensus: A consensus is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record keeping and other things.
- Distributed ledger: A distributed ledger is the shared database in the blockchain network that stores the transactions, such as a shared file that everyone in the team can edit. In most shared text editors, anyone with editing rights can delete the entire file. However, distributed ledger technologies have strict rules about who can edit and how to edit. You cannot delete entries once they have been recorded. Smart contracts: Companies use smart contracts to self-manage business contracts without the need for an assisting third party. They are programs stored on the blockchain system that run automatically when predetermined conditions are met. They run if-then checks so that transactions can be completed confidently. For example, a logistics company can have a smart contract that automatically makes payment once goods have arrived at the port.
- Public key cryptography: Public key cryptography is a security feature to uniquely identify participants in the blockchain network. This mechanism generates two sets of keys for network members. One key is a public key that is common to everyone in the network. The other is a private key that is unique to every member. The private and public keys work together to unlock the data in the ledger.

1.3. Data Storage and Management

- Header: It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.
- Previous Block Address/ Hash: It is used to connect the i+1th block to the ith block using the

hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

- Timestamp: It is a system that verifies the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.
- Nonce: A nonce number which used only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.
- Merkel Root: It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

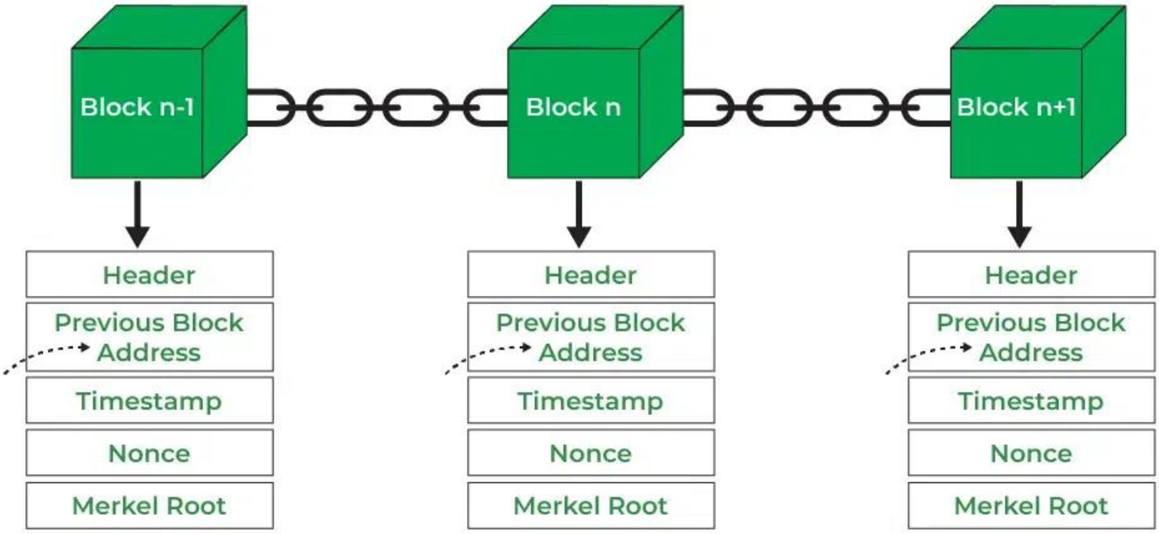

Fig 2: Blockchain Structure. Adapted from updated on 23 Jul, 2025
Source: *https://www.geeksforgeeks.org/ethical-hacking/blockchain-structure/*

2. Types of Blockchain

Blockchain technology can be categorized into four principal types: public, private, consortium, and hybrid blockchains. Each type differs in its level of decentralization, accessibility, governance structure, and security properties, depending on the intended use case and trust requirements (Yaga et al., 2018; Zheng et al., 2018).

Fig 3: Public Blockchain. Adapted from by Oreoluwa F. on 12 May 2024
Source: *https://vezgo.com/blog/public-vs-private-blockchain/*

2.1. Public Block chain

Fig 4: Private Blockchain. Adapted from by Oreoluwa F. on 12 May 2024

Source: *vezgo.com/blog/public-vs-private-blockchain/*

A public blockchain functions as a fully decentralized and permissionless network in which any individual can join, validate transactions, and participate in consensus operations. This model promotes transparency, openness, and collective validation without reliance on a central authority (Nakamoto, 2008; Swan, 2015). Transactions within a public blockchain—such as those in Bitcoin or Ethereum are transparent and immutable, meaning that once blocks are verified, their data cannot be altered. All nodes in a public blockchain maintain a complete copy of the distributed ledger, enabling peer-to-peer verification and ensuring trust through cryptographic consensus mechanisms. Because there is no single controlling entity, public blockchains foster an open ecosystem resistant to censorship or unilateral control (Narayanan et al., 2016).

2.2. Private Blockchain

A private blockchain, also known as a permissioned blockchain, restricts participation to authorized users and is typically governed by a single organization (Zheng et al., 2018). Access control mechanisms determine who can read, validate, and write transactions. This model is most common in enterprise environments where confidentiality and performance are prioritized over openness (Yaga et al., 2018). Since the network authority approves participants and their roles, private blockchains allow higher throughput and regulatory compliance but introduce an element of centralized trust (Cachin & Vukolić, 2017).

2.3. Consortium Blockchain

A consortium blockchain, also called a federated blockchain, is jointly administered by a group of preselected organizations rather than a single entity (Zheng et al., 2017). It is designed to foster collaboration among multiple institutions, such as financial, governmental, or research organizations, while maintaining partial decentralization. Governance within consortium blockchains is distributed among participants, promoting shared trust and accountability (Swan, 2015). This structure balances the privacy advantages of private blockchains with the transparency features of public blockchains.

2.4. Hybrid Blockchain

A hybrid blockchain integrates components of both public and private blockchains to achieve an optimal balance between data transparency and privacy. This model allows organizations to configure which information remains confidential and which is publicly accessible (Zheng et al., 2018; Yaga et al., 2018). Prominent examples include IBM's Food Trust system and Dragonchain, which apply hybrid models to enhance traceability and data protection. Hybrid blockchains are particularly useful in enterprise applications such as supply chain management, healthcare, and identity verification, where selected transparency strengthens trust while preserving operational confidentiality.

3. Blockchain's Industrial use

Blockchain transforms industries with secure, transparent data management. Here are key applications:

1. Supply Chain: Tracks goods from source to delivery, cutting fraud in food, pharma, and luxury items. IBM Food Trust enables seconds-fast traceability
2. Finance: Speeds cross-border payments and trade via smart contracts, skipping middlemen. JPMorgan's Onyx handles billions daily, slashing costs
3. Healthcare: Secures patient records with privacy controls and verifies drug authenticity to fight counterfeits
4. Asset Tokenization: Turns real estate or commodities into tradeable digital tokens for fractional ownership and liquidity
5. Energy: Powers peer-to-peer renewable trading with automated billing and grid checks via smart meters
6. Sustainability: Tracks carbon credits and ESG data transparently, aiding compliance and emissions reporting
7. Elections: Prevents rigging with immutable voter ledgers for registration and verifiable public vote records

4. Limitations of Blockchain Technology

While blockchain technology offers significant advantages in decentralization and data integrity, its practical deployment faces substantial technical, organizational, economic, and regulatory constraints. These limitations must be critically evaluated when considering blockchain adoption in industrial or enterprise applications.

4.1. Technical Limitations

4.1.1. Scalability Constraints

Blockchain networks, particularly public permissionless systems, exhibit limited transaction throughput due to consensus requirements across distributed nodes. Bitcoin processes approximately 7 transactions per second (TPS), and Ethereum around 15-30 TPS, far below Visa's capacity of 24,000 TPS. Solutions such as sharding and layer-2 protocols remain experimental and introduce complexity.

4.1.2. High Energy Consumption

Proof-of-Work (PoW) consensus mechanisms demand immense computational resources. Bitcoin's annual energy consumption rivals that of mid-sized countries like Argentina, generating significant carbon emissions and raising sustainability concerns. Even Proof-of-Stake (PoS) alternatives, while more efficient, require substantial infrastructure.

4.1.3. Interoperability Challenges

Heterogeneous blockchain protocols lack standardized communication interfaces, hindering data exchange between networks. Cross-chain bridges remain vulnerable to exploits, as evidenced by over $2 billion in losses from bridge hacks between 2021-2025.

4.2. Organizational and Economic Barriers

4.2.1. Implementation Costs

Initial deployment involves high capital expenditures for infrastructure, integration, and skilled personnel. Enterprise blockchain projects often exceed budgets by 50-100%, with ongoing maintenance costs further eroding ROI. Small and medium enterprises face particular barriers due to resource constraints.

4.2.2. Governance Complexity

Permissioned blockchains require sophisticated access control and decision-making frameworks. Consortium models introduce coordination challenges among multiple stakeholders, often resulting in stalled projects or centralized drift that undermines decentralization benefits.

4.3. Regulatory and Legal Constraints

4.3.1. Data Protection Conflicts

Blockchain's immutability conflicts with regulations like the EU's General Data Protection Regulation (GDPR), which mandates data rectification and erasure ("right to be forgotten"). Off-chain solutions or selective disclosure mechanisms remain technically immature.

4.3.2. Regulatory Uncertainty

Absence of global standards creates compliance risks across jurisdictions. Smart contracts may not receive legal recognition equivalent to traditional agreements, exposing parties to enforcement uncertainties in disputes.

4.4. Security and Privacy Limitations.

4.4.1. Smart Contract Vulnerabilities

Code-based contracts are susceptible to bugs and exploits. The 2016 DAO hack resulted in $60 million in losses due to reentrancy attacks, highlighting ongoing risks despite formal verification tools.

4.4.2. 51% Attack Risk

Public blockchains remain vulnerable to majority hash power control, enabling double-spending or transaction censorship. Smaller networks face heightened risks, with several altcoins experiencing such attacks.

4.5. Storage and Performance Issues

4.5.1. Data Bloat

Distributed ledgers require all full nodes to store complete transaction histories, leading to rapid storage growth. Bitcoin's blockchain exceeds 500 GB as of 2026, imposing bandwidth and storage burdens on participants.

4.5.2. Latency

Finality times vary from minutes (PoW) to seconds (modern PoS), unsuitable for high-frequency trading or real-time IoT applications requiring sub-second confirmation.

5. Conclusion

Blockchain technology represents a paradigm shift in distributed data management, characterized by its decentralized architecture, cryptographic immutability, and consensus-driven validation mechanisms. By structuring transactions into chronologically linked blocks, it establishes a tamper-resistant ledger that ensures data integrity across diverse applications, ranging from financial systems to supply chain provenance tracking,. The incorporation of smart contracts further extends blockchain's utility, enabling autonomous execution of complex agreements and reducing reliance on intermediaries. Empirical evidence from sectors such as finance (e.g., JPMorgan's Onyx), healthcare (patient data interoperability), and logistics (IBM Food Trust) demonstrates measurable improvements in transparency, efficiency, and trust. Core attributes including distributed storage, peer-to-peer governance, and cryptographic security position blockchain as a robust alternative to centralized systems, mitigating vulnerabilities such as single points of failure and opaque auditing.

Nevertheless, realizing blockchain's full potential requires addressing persistent limitations, including scalability constraints, energy-intensive consensus protocols, regulatory uncertainties, and interoperability challenges. Ongoing research into layer-2 scaling solutions, energy-efficient consensus mechanisms (e.g., Proof of Stake), and standardized protocols will be essential to overcome these barriers. As institutional adoption accelerates—evidenced by enterprise consortia and governmental initiatives—blockchain is poised to reshape data governance frameworks across industries. Future advancements will depend on interdisciplinary collaboration to balance innovation with practical deployment constraints, ensuring this technology's sustainable evolution and long-term viability.

References

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. 2017 IEEE Int. Congress on Big Data (BigData Congress), 2017, pp. 557-564.

[4] C. Cachin and M. Vukolifá, "Blockchain consensus protocols in the wild," arXiv preprint arXiv:1707.01873, 2017

[5] D. Yaga, P. Mell, N. Roby, and K. Scarfone, Blockchain Technology Overview (NISTIR 8202), National Institute of Standards and Technology, 2018.

[6] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.

[7] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in Proc. 19th IEEE Int. Conf. on Intelligent Transportation Systems, 2016, pp. 2663-2668.

[8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[9] F. T. Pilkington, "Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations, F. X. Olleros and M. Zhegu, Eds. Cheltenham, U.K.: Edward Elgar, 2016, ch. 11, pp. 225-253.

[10] M. Androulaki et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSys Conf., Porto, Portugal, 2018, pp. 1-15.

[11] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," arXiv preprint arXiv:1906.11078, 2019

[12] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: An overview," PeerJ Comput. Sci., vol. 9, Art. no. e1705, 2023.

[13] Sunkara, S. K. (2025). Leveraging Ai, Iot, And Blockchain For Scalable Digital Transformation In Post-Harvest Supply Chains: A Multi-Sector Approach To Enhancing Efficiency And Traceability (Vol. 26, Issue 7, Pp. 2757–2766)