Rudra Rai , 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Blockchain Technology: Evaluation Across Security, Scalability, Privacy and Governance

Rudra Rai, Krishnakant Tripathi, Priya Pandey
School of Computer Science and Engineering Galgotias University
Greater Noida, Uttar Pradesh, India,

Abstract- Blockchain is becoming an approachable data platform with several stakeholders having a shared history of transactions without being owned by an individual. The fundamental concepts of cryptographic hashing, peer-to-peer communication, and agreement protocols are sufficiently documented, and a lot of current research focuses on performance, security, privacy, and governance individually rather than as interacting dimensions. Recent blockchain research publications and deployments were structured based on a four-axis perspective that follows the dynamics of a system in terms of security, scalability, privacy, and governance. This lens was applied to consent mechanisms including proof-of-work, proof-of-stake, and practical Byzantine fault tolerance, and to techniques such as sharding and layer-2 that are designed to enhance throughput. Basic throughput calculations using reported block sizes, transaction sizes, and block intervals indicate that configuration limits are usually much larger than the transaction rates achieved in practice, implying that protocol overheads and network behaviour require a major share of the budget. A survey of attacks and defences indicates that increases in speed and programmability often expand the attack surface at the consensus and smart contract layers, which motivates the development of better analysis and monitoring tools. The results are applied to draw design insights for domains of finance, supply chains, healthcare, identity, and smart city platforms, and to highlight remaining problems in benchmarking and cross-chain coordination. A practical mapping of major blockchain platforms, namely Bitcoin, Ethereum, and Hyperledger Fabric, onto the four-axis framework was also provided to demonstrate its utility for platform comparison and selection.

Keywords: Blockchain, consensus mechanisms, scalability.

I. INTRODUCTION

Blockchains are shared ledgers or append-only systems in which many parties can add information in such a way that anyone can identify if an attempt has been made to alter the data. Digital signatures, hashing functions, and peer-to-peer networking are used to allow nodes to share blocks and transactions while a consensus mechanism determines which block to add next. These are the fundamental components of blockchain technology. With the growing interest in blockchain technology among both industry and research communities, there are increasing concerns regarding scalability, power consumption, and interoperability between different blockchain systems [1], [3].

A. Comparative Analysis with Existing Works

A large number of survey articles and case studies now exist covering consensus algorithms, blockchain architecture, and applications across various sectors [1], [4], [5]. Nonetheless, most discussions focus on security, scalability, privacy, and governance as independent issues rather than examining how a design choice beneficial to one axis may negatively affect another [6], [9]. A protocol that is more efficient may alter attack vectors or create regulatory challenges, and a privacy-enhancing method can make regulation and auditability more difficult [6], [10]. An organised system for presenting the relationships between these four dimensions through both qualitative description and quantitative indicators is therefore useful for comparing platforms and deployment configurations.

B. Motivation

Classical information systems rely on databases owned and controlled by a single organisation, which establishes definite points of control but simultaneously introduces definite points of failure and censorship. Blockchain-based solutions attempt

to distribute trust among multiple nodes such that unilateral manipulation of records is difficult to complete without detection, while applications are able to operate at reasonable speed and meet legal demands [1], [3]. Understanding how various architectures balance these goals is important before implementing them in sensitive application domains.

C. Contributions of the Paper

This paper makes several contributions to the structured understanding of blockchain systems. First, it presents a succinct overview of public, consortium, and private blockchain implementations that displays the relationship between deployment type and its effect on consensus, access control, and governance schemes [1], [3]. Second, it introduces a four-dimensional assessment framework that classifies systems and research contributions based on security, scalability, privacy, and governance as organising dimensions [1], [8].

Third, it maps this framework to recent literature on consensus mechanisms and scalability schemes, connecting simple throughput characterisations with reported performance and security consequences [6], [10]. Fourth, it provides domain-specific discussion covering finance, supply chains, healthcare, identity, and smart cities, alongside open questions on benchmarking and cross-chain interoperability [1]–[3]. Finally, it offers a practical mapping of major blockchain platforms, including Bitcoin, Ethereum, and Hyperledger Fabric, onto the four-axis framework to demonstrate its utility for platform comparison and selection.

D. Organisation of the Paper

Section II surveys related literature on consensus mechanisms, performance measures, scalability architectures, privacy, and security. Section III details how studies were collected and classified as well as the evaluation scheme. Section IV presents the conceptual architecture, interprets the performance equations, and summarises security and application-level observations. Section V discusses the limitations of the research and outlines directions for future work. Section VI provides concluding statements.

E. Public, Consortium, and Private Blockchains

Blockchain deployments can be divided into public, consortium, and private types depending on who is permitted to read data, submit transactions, and participate in consensus. Permissionless public systems allow any entity to act as a validating node, promoting transparency at the cost of scalability and privacy. Validation rights in consortium systems are managed by a group of known organisations, while in private environments a single organisation controls membership and access. These high-level decisions strongly influence the selection of consensus protocols and the nature of governance and access control in practice [1], [3].

II. LITERATURE SURVEY

Initial research focused on digital currencies and the Bitcoin model, employing proof-of-work and block rewards to motivate miners to extend the chain. Smart contract platforms such as Ethereum extended this concept to general-purpose computation and decentralised applications, in which logic unrelated to currency transfers can be executed on-chain. Subsequent surveys cover characteristics such as decentralisation, immutability, transparency, traceability, and programmability, associating these properties with applications that require auditable or tamper-evident logs [1], [3].

A. Consensus Mechanisms in Literature

A broad range of consensus protocols have been suggested and studied in the blockchain context [4], [5]. Proof-of-work employs computational puzzles to control block generation, making chain rewriting costly, whereas proof-of-stake and related schemes select validators according to their economic stake, reducing energy consumption at the expense of different economic and security assumptions [1], [4]. Protocols based on the practical Byzantine fault tolerance family are typically utilised in permissioned networks whose validators are known and limited in number [4]. Comparative studies evaluate these families based on throughput, latency, and resilience to various attack scenarios [6]. Table I summarises the broad characteristics of common mechanisms and their typical deployment scenarios.

B. Quantitative Performance Metrics

The most common performance discussion topics are the number of transactions a system can complete per unit time, the length of time required to receive confirmations, and the computing and communication resources required [6]. Throughput is commonly expressed in transactions per second (TPS):

$$\mathrm{TPS} = \frac{N_{\mathrm{committed}}}{\Delta t} \quad (1)$$

where Ncommitted is the number of transactions recorded in a time window of duration Δt [6], [10]. For a given block size
B, average transaction size S, and block interval Tb, a simple upper bound on throughput is:

$$\mathrm{TPS}_{\max} \approx \frac{B/S}{T_b}, \quad (2)$$

which illustrates how configuration parameters constrain potential performance [10].

TABLE I: Common Blockchain Consensus Mechanisms

Mechanism	Typical Setting	Indicative Properties
PoW	Public, permissionless	High security, high energy use, low TPS [1]
PoS	Public, permissionless	Lower energy, stake-dependent security [4]
DPoS	Public, semi-permissioned	Higher TPS, delegated validators [4]
PBFT	Consortium, private	Low latency, limited validator set [4]

TABLE II: Representative Blockchain Application Domains

Domain	Typical Objective	Example
Finance	Secure settlement and programmable assets	DeFi [1]
Supply chain	Provenance and anti-counterfeiting	Food traceability [1]
Healthcare	Controlled sharing of medical records	EHR sharing [1]
Identity	Self-sovereign and verifiable credentials	DID systems [1]
Smart cities	Trusted data sharing for IoT and services	Sensor data markets [1], [3]

C. Scalability and Layered Designs

In several systems, a significant portion of nodes serve all transactions, which constrains throughput and extends confirmation times [1]. This limitation motivates sharding, which divides the network into subsets enabling parallel transaction processing, and layer-2 techniques such as payment channels and rollups, which off-load most interactions and anchor summary data on the base layer. Such approaches can provide substantial capacity improvements, yet they introduce protocol complexity and create new failure modes that must be understood and mitigated [7].

D. Privacy and Regulatory Perspectives

Privacy and regulation are critical considerations when blockchains are applied to personal or commercially sensitive information. Permanent storage of transactional information in public ledgers may conflict with data minimisation mandates and the right to erasure, motivating investigation into mixers, ring signatures, and zero-knowledge proofs that conceal specific information without invalidating the integrity of outputs. In permissioned systems, sensitive data is often stored off-chain, and fine-grained access control together with auditable key management is used to balance transparency against privacy [1], [3].

E. Security and Smart Contract Vulnerabilities

Although ledger-level integrity is generally high in blockchain systems, they remain vulnerable to several categories of threats. At the consensus layer, majority attacks, selfish mining, or stake-concentration attacks can affect transaction ordering; at the application layer, logic errors, state bugs, or reentrancy vulnerabilities in smart contracts can be exploited. Security studies classify risks into categories covering network behaviour, consensus manipulation, wallet and key management, and social engineering, and recommend combinations of formal techniques, code analysis tools, secure development practices, and operational monitoring [9].

F. Application Domains in Literature

Numerous industries have been identified as potential beneficiaries of blockchain-based

infrastructure, each with distinct requirements and limitations. Representative areas include financial settlement, traceable supply chains, health record sharing, digital identity management, and smart city services, as summarised in Table II [1], [3].

III. METHODOLOGY

The paper is based on qualitative reading of research articles as well as mathematical calculations using published performance metrics of blockchain systems, in order to map blockchain systems onto the four-axis model. Peer-reviewed works are supplemented by selected analyst and market reports that provide an indicative picture of usage trends and projected growth [1], [2].

Algorithm 1 Classification of Studies Along Evaluation Axes

Algorithm 1 Classification of Studies Along Evaluation Axes

Require: Set of publications P

1: **for all** $p \in P$ **do**
2: Extract blockchain type, consensus family, application domain
3: Identify reported metrics (e.g., TPS, latency, energy, privacy guarantees)
4: Choose primary axis from {security, scalability, privacy, governance}
5: Note any additional axes that are explicitly discussed
6: **end for**
7: Combine observations to infer common patterns and trade-offs

A. Review Procedure

The literature review followed three steps. In the first step, recent surveys and overview papers presenting the fundamentals of blockchain, consensus families, scalability, and typical usage scenarios were collected [1], [4], [5]. In the second step, common architectural designs, consensus types, security models, and trade-offs described by the authors were identified and recorded [1], [8]. In the third step, the derived insights were connected to application areas such as finance, supply chains, healthcare, and smart cities to understand how requirements vary across domains [1], [3].

B. Data Extraction and Synthesis

For each paper meeting the selection criteria, the deployment type (public, consortium, or private), consensus family, transaction or state model, and primary application focus were noted [1], [4]. The synthesis was deliberately qualitative, seeking to identify patterns, unresolved issues, and common trade-offs rather than producing formal statistical meta-analysis. Market size estimates, growth rates, and adoption trends from industry reports were treated as rough estimations rather than precise projections [2].

C. Market and Adoption Data

Analysts project that total market expenditure on blockchain technologies may increase from approximately USD 19.7 billion in 2024 to significantly more than USD 2,450 billion by 2034, representing a high compound annual growth rate. These figures should be treated with caution, but they are consistent with the observation that blockchain concepts are being explored across an increasing number of industries [2], [3].

D. Evaluation Framework

In order to maintain coherence, studies were interpreted through four dimensions: security, scalability, privacy, and gover-nance. Each paper was assigned a primary axis according to its key contribution, and secondary axes were noted where they were substantively addressed [1], [3]. Security encompasses consensus robustness and smart contract soundness; scalability encompasses throughput, latency, and resource use; privacy encompasses what information is disclosed or concealed and under which access controls; and governance addresses how proposals to amend protocol or configuration are presented and adopted [6], [8]. This classification was carried out in accordance with Algorithm 1.

E. Merkle Tree and Hashing Model

In many blockchains, transactions are organised into a block by placing them in a Merkle tree whose root constitutes a hash of the block contents. In a balanced tree with n transactions, padded to the next power of two where applicable, the approximate number of levels L is given by:

$$L \approx \lceil \log_2 n \rceil. \quad (3)$$

Because this is a logarithmic rather than linear relationship, evidence that a specific transaction occurred in a block remains compact even when many transactions are stored, which is a primary reason such structures are prevalent in distributed ledgers [11].

IV. RESULTS AND DISCUSSION

This section describes the generic architecture used as a reference point, illustrates how the performance expressions can be interpreted, and identifies the key trade-offs and security observations reported in the reviewed literature [1], [6].

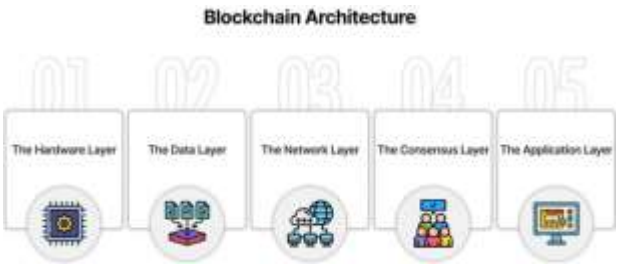

Fig. 1: Conceptual blockchain architecture with data, network, consensus, and application layers and links to external storage.

A. Conceptual Architecture

The simplified layered architecture considered in this study is illustrated in Fig. ??. The bottom layer is the data layer, which encodes blocks, transactions, hashes, and signatures. Above it, the network layer handles message passing between nodes. The consensus layer guarantees that blocks are correctly added to the chain, whether through PoW, PoS, PBFT, or their variants. The application layer hosts smart contracts and other domain-specific logic that makes use of the ledger. External systems and off-chain databases are typically connected through oracles or APIs, especially in permissioned deployments where integration with external infrastructure is necessary [1], [3].

B. Interpretation of Performance Metrics

The definition given in (1) reflects the rate at which finality is actually achieved under real network and protocol conditions, while (2) provides a crude upper bound that depends solely on configuration parameters. In practical proof-of-work systems, actual throughput is often significantly lower than this bound due to strict block-size choices, propagation latency, and the need to control fork rates [6], [10]. In PBFT-type permissioned systems, reported performance may approach the configuration bound with moderate numbers of validators, but communication cost grows with the validator count [4], [6].

C. Performance and Trade-offs

The surveyed work consistently reveals a picture in which throughput, latency, energy cost, and decentralisation are mutually constrained [4], [6]. Proof-of-work constructions offer high censorship resistance and robustness under varied network conditions at the expense of low TPS and high energy use. Proof-of-stake proposals consume fewer resources and can reduce confirmation times, but shift security considerations towards stake distribution and long-term attack models. PBFT and its extensions offer low latency within constrained validator sets but do not scale well to large, open networks [1], [4]. Sharding schemes and layer-2 protocols are designed to push a portion of work off the base layer or to distribute workloads among parallel shards, at the cost of increased protocol complexity [6], [7]. Table III lists the core blockchain features most frequently referenced in the surveyed literature and their primary benefits from an application design perspective [1], [3].

D. Practical Platform Mapping

Bitcoin's proof-of-work consensus is oriented towards censorship-resistant and secure transactions but results in low through-put of approximately three to seven transactions per second and high energy consumption. Ethereum's upgradeable model supports programmable applications through smart contracts but introduces additional attack vectors at the application layer, making formal verification and auditing essential for any production deployment. The planned transition to proof-of-stake under Ethereum 2.0 is expected to improve scalability and reduce energy consumption while retaining the existing security model. Hyperledger Fabric offers an alternative approach designed for enterprise environments where all participants are known and bound by legal agreements.

Its permissioned architecture supports throughput of approximately 3,500 transactions per second and enables fine-grained access control through a modular consensus design, though it provides less

censorship resistance than public chains. In summary, this comparison yields an evaluation framework in which the choice of platform is guided by

TABLE III: Key Blockchain Features and Benefits

Feature	Primary Benefit
Decentralisation	Reduces single points of failure and central control [1].
Immutability	Makes undetected modification of past data harder [1].
Transparency	Supports auditable histories for authorized parties [1].
Programmability	Enables smart contracts and custom logic [1].
Traceability	Helps implement end-to-end provenance tracking [1], [3].

the requirements of the application: Bitcoin is most appropriate for monetary applications demanding maximum censorship resistance, Ethereum for decentralised applications requiring programmability, and Hyperledger Fabric for enterprise contexts in which throughput and privacy are the primary concerns.

E. Security Analysis

The classification outcomes highlight that security challenges span multiple layers and are frequently interdependent. At the network level, isolation or flood attacks may cause nodes to develop a distorted view of the chain state. At the consensus level, attackers may seek majority control of computational or economic resources, or exploit protocol specifics to influence block selection. At the application level, coding bugs in smart contracts or incorrect use of libraries may result in fund losses or unintended transfers even when the underlying ledger operates correctly [8], [9]. Proposed countermeasures include formal modelling and verification of critical contracts, the use of static and dynamic analysis tools during development, hardened key management through hardware security modules or multi-signature schemes, and the deployment of on-chain monitoring infrastructure [8], [9].

F. Impact on Application Design

Examined across domains, the four-axis framework reveals why different application areas make different architectural decisions. Financial applications typically prioritise censorship resistance and settlement finality and are often willing to accept greater latency and cost, whereas supply chain systems generally require predictable throughput and verifiable control among a known group of organisations. Healthcare and identity management applications frequently impose strict privacy and consent requirements that lead to hybrid designs in which only references or cryptographic commitments are stored on-chain while the data itself resides in off-chain storage [1], [3]. In smart city contexts, resource-constrained devices and heterogeneous communication networks impose additional requirements that drive interest in lightweight protocols or layer-2 implementations that reduce on-chain load [3]. The framework thus provides a structured basis for discussing these trade-offs when evaluating new use cases.

V. LIMITATIONS AND FUTURE WORK

This study has several limitations. It relies on interpretation of existing publications rather than controlled experiments comparing platforms under identical conditions. Reported throughput and latency values come from studies using different workloads and environments, making direct comparisons difficult. Market and adoption data drawn from analyst reports are inherently speculative and should be treated accordingly [1], [2], [6]. Future work could extend the four-axis framework into a concrete benchmarking infrastructure measuring performance and security metrics across implementations under varied and controlled conditions [6].

Additional research directions include systematic analysis of cross-chain protocols, improved understanding of governance mechanisms in permissionless systems, and deeper investigation of interactions between blockchain designs and emerging technologies including Internet of Things applications, artificial intelligence components, and edge computing architectures [1], [3]. Standardised

benchmarking methodologies and formal models for reasoning about cross-chain security would help advance responsible deployment of blockchain technology across sensitive domains.

A. Standardised Benchmarking Framework

Future work should develop a concrete benchmarking infrastructure that measures performance and security metrics across multiple blockchain implementations under controlled and standardised conditions. Such a framework should specify standard workload definitions representing realistic transaction patterns for different application domains, network topology configura-tions reflecting various deployment scenarios including cloud, edge, and hybrid environments, metrics collection methodologies that ensure reproducibility and comparability, and stress testing protocols to evaluate behaviour under adversarial conditions and peak loads.

B. Cross-Chain Interoperability

As blockchain deployments proliferate across domains, the need for secure cross-chain communication becomes critical. Research should address formal security models for cross-chain protocols including atomic swaps and relay mechanisms, standardised interfaces enabling heterogeneous chains with different consensus mechanisms to exchange assets and data, trust models for bridge validators and oracle networks, and the performance implications of cross-chain operations on individual chain throughput and latency.

VI. CONCLUSION

This paper presented a framework built on four primary dimensions, namely security, scalability, privacy, and governance, through which blockchain systems can be compared and evaluated. The framework was applied to recent work on consensus mechanisms, scalability solutions, and application domains to produce a structured synthesis of the literature. The analysis showed that enhancements in throughput and flexibility frequently introduce new categories of risk, particularly at the consensus and smart contract layers, and that the appropriate trade-offs are highly dependent on the context of the application. Public blockchains such as Bitcoin and Ethereum offer strong censorship resistance and programmability at the cost of throughput and energy use, while permissioned systems such as Hyperledger Fabric achieve higher transaction rates and finer access control at the cost of reduced openness. Across application domains spanning finance, supply chains, healthcare, identity management, and smart cities, the four-axis framework proved useful for explaining why different architectural choices are made and what compromises they entail. The study is subject to limitations arising from the use of heterogeneous published benchmarks rather than controlled experiments, and from the speculative nature of market projections. Further efforts in standardised benchmarking, cross-chain interoperability, and domain-specific design are therefore important prerequisites for the responsible deployment of blockchain technology in sensitive sectors.

DECLARATIONS

The authors declare that there are no conflicts of interest regarding the publication of this article. No external funding was received for this study. All sources used in this paper are appropriately cited.

REFERENCES

1. S. Dong, Y. Zhang, X. Zhang, and X. Li, "Blockchain technology and application: an overview," Digital Communications and Networks, 2023. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC10703090/
2. Fact.MR, "Blockchain technology market share & statistics 2034," 2024. [Online]. Available: https://www.factmr.com/report/ blockchain-technology-market
3. ICVL, "Blockchain technology: architecture, consensus, and future trends," in Proc. ICVL 2024, 2024. [Online]. Available: https://icvl.eu/documents/ 107/ICVL-2024.pdf
4. P. Khobragade and S. Patil, "Blockchain consensus algorithms: a survey," in Proc.

International Conference on Blockchain Applications, 2022. [Online].
5. Available: http://dspace.nitrkl.ac.in/dspace/bitstream/2080/3720/1/2022 ICBA PKhobragade Blockchain.pdf
6. J. Liu, "A comprehensive survey of blockchain consensus mechanisms," Computer Networks, 2025. [Online]. Available: https://www.sciencedirect.com/ science/article/abs/pii/S1389128625006280
7. B. Bhavana et al., "Comparative evaluation and simulation of blockchain consensus," 2025. [Online]. Available: https://www.nature.com/articles/ s41598-025-27431-w
8. S. Shirodkar, K. Kulkarni, R. Khanjode, S. Kohle, P. Deshmukh, and P. Patil, "Layer 2 solutions to improve the scalability of blockchain," in Proc. 2022 5th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2022, pp. 54–57, doi: 10.1109/ICAST55766.2022.10039486.
9. D. Liu, "Blockchain smart contract security: threats and mitigation," 2025. [Online]. Available: https://dl.acm.org/doi/10.1145/3769013
10. A. AlFaw, W. Elmedany, and M. S. Sharif, "Blockchain vulnerabilities and recent security challenges: a review paper," in Proc. 2022 International Conference on Data Analytics for Business and Industry (ICDABI), Sakhir, Bahrain, 2022, pp. 780–786, doi: 10.1109/ICDABI56818.2022.10041611.
11. Hashlock, "Understanding TPS: which blockchains are the fastest?," 2025. [Online]. Available: https://hashlock.com/blog/ understanding-tps-which-blockchains-are-the-fastest
12. O. Kuznetsov, "Merkle trees in blockchain: a study of collision probability and path length," 2024. [Online]. Available: https://arxiv.org/pdf/2402.04367.pdf