1_similarity 94 Sumarhadi

by Turnitin No Repository

Submission date: 19-Jun-2026 05:48PM (UTC+0900)
Submission ID: 2985978313
File name: 1_similarity_94_Sumarhadi.docx (309.91K)
Word count: 6385
Character count: 41798

Architectural and Fundamental Analysis of Blockchain: A Comparative Overview of Working Mechanisms, Tokenization, and Data Decentralization

Dedy Sumarhadi[1,2], Sunardi[3], Imam Riadi[4]
Polteknik Mardira Indonesia, Indonesia[1]
Universitas Ahmad Dahlan, Indonesia[2,3,4]
dedysumarhadi@poltekmi.ac.id[1], 2537083011@webmail.uad.ac.id[2], sunardi@mti.uad.ac.id[3], imam.riadi@is.uad.ac.id[4]

Abstract

Blockchain technology has evolved from a nascent peer-to-peer payment system into a paradigm-shifting digital trust infrastructure, fundamentally challenging conventional centralised models. However, a deep understanding of the fundamental technical aspects behind the popularity of crypto assets remains limited. This study aims to: (1) analyse the fundamental architecture of blockchain; (2) evaluate tokenisation mechanisms; and (3) conduct a comparative analysis of its characteristics against traditional database systems. The research employs a qualitative descriptive method utilising a Systematic Literature Review (SLR) approach to synthesise technical literature published between 2023 and 2025. The analysis focuses on consensus mechanisms, the architectural transition from monolithic to modular systems (Layer-2 scaling), and the measurement of decentralisation using the Nakamoto Coefficient. The results indicate that: (1) blockchain offers distinct advantages in data integrity (immutability) and censorship resistance through a distributed append-only ledger structure, standing in sharp contrast to the CRUD (Create, Read, Update, Delete) model of relational databases; and (2) recent innovations such as Zero-Knowledge Proofs and Optimistic Rollups serve as critical solutions to the "Blockchain Trilemma" (balancing scalability, security, and decentralization). This study concludes that blockchain is not an absolute replacement for conventional databases, but rather a specialised solution for ecosystems that require high transparency and "trustless" interactions without a central authority.

Keyword: *Blockchain Architecture, Distributed Ledger Technology (DLT), Tokenomics, Layer-2 Scalability, Relational Database.*

INTRODUCTION

Phenomena and Gap Analysis

Blockchain technology has evolved significantly from a mere peer-to-peer payment system into a new paradigm of digital trust infrastructure, challenging conventional centralized models. This phenomenon is marked by the global adoption of crypto assets; however, a deep understanding of the fundamental technical aspects behind this popularity remains limited. Theoretically, there is a knowledge gap: blockchain is often viewed solely as a financial instrument, ignoring its architectural distinction as a distributed, append-only ledger compared to traditional **CRUD** (Create, Read, Update, Delete) databases. Furthermore, a research gap exists in the current literature. While many studies focus on market volatility or specific implementations, there is a lack of a comprehensive comparative analysis that evaluates the architectural transition from monolithic to modular systems and measures decentralization using quantitative technical metrics, such as the Nakamoto Coefficient, against traditional database standards.

Summary of Previous Studies

Recent studies have addressed specific components of this technology, (Qi et al., 2024). Provided a comprehensive survey on Bitcoin Layer Two (L2) solutions, highlighting scalability mechanisms to overcome mainnet

limitations. Meanwhile, (Ovezik et al., 2025). Focused on the methodology for measuring blockchain decentralization, emphasizing the importance of accurate metrics in distributed systems. Additionally, (Hafid et al., 2023). Aanalyzed blockchain scalability solutions and offered a taxonomy of on-chain and off-chain scaling approaches. Despite these valuable insights, there is still a need for a study that synthesizes these elements fundamental architecture, tokenization mechanisms, and decentralization metrics into a holistic comparison with the centralized database systems that currently serve as the industry standard.

Problem Statement and Research Objectives

Based on the background above, this study aims to analyze the fundamental architecture of blockchain, evaluate tokenization mechanisms, and compare its characteristics with traditional databases. Specifically, the research questions formulated in this study are:

1. How do the fundamental architecture and operational mechanisms of Blockchain technology compare to those of traditional centralized databases?
2. How do tokenization mechanisms and distributed ledger structures contribute to data integrity (immutability) and censorship resistance?
3. How has the blockchain architecture evolved from monolithic to modular (Layer-2) systems, and what is the level of decentralization when measured by the Nakamoto Coefficient?

While traditional centralized databases prioritize efficiency at the expense of transparency and security, blockchain technology offers a decentralized alternative, often constrained by the Blockchain Trilemma. The subsequent evolution from monolithic to modular (Layer-2) architectures aims to resolve these scalability bottlenecks, yet it simultaneously necessitates a more rigorous assessment of data integrity and actual decentralization. Consequently, without clear quantitative metrics such as the Nakamoto Coefficient, the true degree of decentralization in these evolving systems remains subjective and difficult to verify.

Blockchain and Working Mechanisms

In the current information age, the greatest challenge in data exchange is trust. Fundamentally, blockchain is a decentralised, distributed ledger that records transactions across multiple computers so that records cannot be altered retroactively.

Unlike conventional banking systems that rely on a central authority, blockchain distributes copies of data to all nodes within the network, thereby eliminating single points of failure, (Li et al., 2025).

Its working mechanism relies on a linear data structure composed of interconnected blocks. The uniqueness of this technology lies in the manner in which data is encapsulated and secured, as outlined in the following points; **Block Structure**, bach block contains a batch of transactions, a timestamp, and two crucial cryptographic components: the hash of the current block and the hash of the previous block. **Hash Function,** the use of cryptographic algorithms (such as SHA-256) ensures that any alteration to a block's data will completely change its hash value, thereby invalidating all subsequent blocks in the chain.(Dattaprasad Patil & Vijaya Bhosale, 2023).

It is this mathematical linkage that establishes the property of immutability. If an attacker attempted to alter a single historical transaction, they would be required to recalculate the hash of that specific block and all subsequent blocks across the majority of the network nodes simultaneously a feat considered computationally infeasible with current technology.

In addition to block structure and hashing, another crucial element to comprehend is the Consensus Mechanism. Given the absence of a central authority, how does the network collectively validate a new block? The network employs consensus protocols to achieve agreement; Proof of Work (PoW), used by Bitcoin, wherein computers compete to solve complex mathematical puzzles to validate blocks (a process known to be energy-intensive). Proof of Stake (PoS), used by Ethereum (in its latest version), wherein validators are selected based on the quantity of coins they have "staked" or locked within the network (a more energy-efficient alternative), (Fahim et al., 2023).

Blockchain technology has the potential to transform traditional industries through its key features, such as persistence, anonymity, decentralization, and auditability. Let us examine these four pillars; Persistence, once data is recorded in a block and validated, it remains permanent. This is crucial for industries such as Supply Chain management, where the product provenance (history) from factory to consumer must be recorded immutably. Anonymity & Privacy, although transactions are transparent, user identities are often masked (pseudonymized) as cryptographic addresses (public keys). This provides users with a layer of privacy while preserving the ability to verify publicly. Decentralization, by eliminating intermediaries (such as banks or notaries), transaction costs can be significantly reduced, and processing speeds accelerated (for instance, in cross-border payments). Auditability, because every node has an identical copy of the ledger, auditing can be conducted in real time. Regulators or auditors do not need to request data retrieval from the company; they can inspect the blockchain directly, (Andrew, 2024).

Blockchain Characteristics

Blockchain technology emerged as a solution to the issue of trust within the digital realm. Prior to the advent of blockchain, every electronic transaction required a trusted third party (such as a bank or notary) to validate the integrity of the data. Blockchain shifts this paradigm by transferring trust from institutions to mathematical algorithms and distributed networks.

The following are the key characteristics that form the foundation of blockchain; Decentralization, data is not stored on a single central server but is instead replicated across thousands of computers (nodes) worldwide. This eliminates the risk of a single point of failure, (Nakamoto, n.d.). Immutability, blockchain is immutable because once data is validated and recorded in a block, it cannot be altered, deleted, or modified. Each block contains a unique hash that includes the data itself and the hash of the previous block; consequently, any alteration to the data, no matter how minor, will completely change the hash. Furthermore, since blocks are linked via hashes, altering a single block would invalidate the entire chain of subsequent blocks. To alter data, an attacker must control more than 51% of

the network, a feat that is computationally difficult and prohibitively expensive, especially in large networks, (Singh, 2025). Consensus Mechanism**,** this is the core of blockchain technology, enabling thousands of computers (nodes) in a decentralized network to agree on a single version of data without a central authority. Without consensus, transactions are invalid, and trust is eroded. Key types of consensus mechanisms include Proof of Work (PoW), where miners compete to solve mathematical puzzles to add blocks (e.g., Bitcoin); Proof of Stake (PoS), where block validation is performed by those who "stake" their coins, which is more energy-efficient than PoW (e.g., Ethereum); and Proof of Authority (PoA), which relies on the identity of verified and reputable validators, making it suitable for private blockchains in educational institutions, (Saminur Islam et al., 2023). Transparency & Auditability, in the blockchain ecosystem, transparency and auditability are the two primary pillars that establish trust without reliance on third parties. Transparency ensures that all transaction data is public or accessible to authorized entities (in private networks), with every alteration openly recorded so that all participants can view data in real time. Auditability, enabled by the immutable and chronological nature of the data, allows auditors to trace transaction history from inception to conclusion, creating a complete audit trail to verify the Authenticity of assets such as certificates or NFTs, (Astawa et al., 2025). Cryptographic Security, cryptographic security is the foundation that renders blockchain secure and trustworthy, safeguarding the system against manipulation. In blockchain, this security relies on three primary mechanisms: hashing, which transforms data into a unique string of characters to maintain data integrity; asymmetric key cryptography, where users possess public and private keys to generate digital signatures; and the digital signature itself, which ensures the transaction originates from the legitimate owner and that data remains unaltered during transmission, thereby guaranteeing non-repudiation, (Lb & Rafi, 2025). **Provenance,** in the context of blockchain and Non-Fungible Token (NFT), provenance refers to the chronological record of ownership and the origin of a digital asset from its creation (minting) to its current owner, (Sheldon, 2022). In the educational domain, such as with NFT certificates or diplomas, provenance functions as a "digital lineage" that cannot be manipulated, ensuring legitimate issuance, recording transaction history with permanent timestamps, and proving asset Authenticity without the need for manual verification, (Alavi et al., 2025). **Programmability,** in blockchain, programmability refers to the capability to embed business logic or code instructions into digital assets or transactions via Smart Contracts. In an educational context, this allows digital assets to be dynamic; for example, NFT diplomas can automatically appear in a student's digital wallet upon the completion of all courses, automatic royalties can be distributed to authors of NFT teaching materials, or certificates can be programmed to be active only if specific conditions are met or to expire automatically after a certain period, (Liu et al., n.d.). **Pseudonymity,** in blockchain, it refers to replacing user identities with pseudonyms or cryptographic wallet addresses, such as Bitcoin or Ethereum addresses, that do not entirely conceal the user's identity. Although activity is

publicly visible (e.g., BTC transactions), the user's real identity is known only to the owner or, if linked to other data (e.g., via KYC processes). Unlike anonymity, which completely hides identity, pseudonymity traces activity to a pseudonym that can be linked to a real-world identity, (Androulaki et al., n.d.).

The Relationship Between Blockchain and Tokens

The relationship between blockchain technology and tokens is often misconstrued as identical. Theoretically, blockchain serves as the foundational infrastructure (Layer-1), whereas tokens are assets or utilities that operate atop it.(Samela Kivilo et al., 2025) This relationship can be analyzed through three primary dimensions: value representation, incentive mechanisms, and innovative contract execution.

Definitions and Distinctions: Native Coins vs. Tokens

In digital asset literature, there exists a fundamental distinction between "Coins" and "Tokens" that is frequently confused in lay usage; **Coins (Native Assets),** these are native assets associated with a specific blockchain protocol (e.g., Bitcoin on the Bitcoin network, Ether on the Ethereum network). Their primary function is to serve as a means of payment for transaction fees (gas fees) and as incentives for miners to maintain network security. **Tokens,** these are digital assets issued upon an existing blockchain (typically utilizing smart contracts, such as the ERC-20 standard on Ethereum). Tokens do not have their own blockchain; instead, they "leverage" the parent chain's infrastructure for transaction validation, (Marin et al., 2023).

According to a recent review by Marin et al. (2023), blockchain tokens are developed through smart contracts to enable the digitization of both virtual and physical assets. These tokens serve diverse functions, ranging from ensuring accountability and traceability in supply chains to facilitating social governance and gamification. Furthermore, the study emphasizes that a token's value is driven by a complex interplay of demand and supply, social incentives, and market conditions, effectively creating new token economies that operate with high transparency and efficiency without traditional intermediaries.

Tokens as Incentive Mechanisms and Tokenomics

One of the most significant innovations of blockchain is the application of Game Theory within distributed systems. Since blockchain operates without a central authority, the network requires a robust mechanism to incentivize thousands of computers (nodes) to validate transactions honestly, (Mssassi & Abou El Kalam, 2024).

It is here that the role of coins and tokens becomes vital through the concept of Tokenomics. Tokenomics encompasses the design of supply, distribution, and token utility to ensure the sustainability of the ecosystem. Blockchain protocols are designed to distribute block rewards in the form of digital assets to nodes that successfully solve cryptographic puzzles (Proof of Work) or those that stake their assets (Proof of Stake).

In the absence of these economic incentives, validators' operational costs would remain uncompensated, rendering the network vulnerable to attacks. According to Bihani (2025), tokenomics serves as a strategic

framework for incentive alignment that ensures the long-term sustainability of decentralized networks. By integrating principles from game theory and behavioral economics, digital tokens align the self-interest of individual participants with the collective goal of network integrity. This mechanism effectively eliminates the need for centralized intermediaries, as the algorithmic design itself incentivizes honest behavior and secures the ecosystem against malicious attacks, (Damodar Bihani et al., 2025).

Tokenization, Smart Contracts, and Decentralized Governance

The integration between blockchain and tokens has intensified with the advent of Smart Contracts. Modern tokens function not merely as a medium of exchange but as programmable money. Through smart contracts, Real World Assets (RWA) can be digitally represented, a process referred to as Tokenization, (Damodar Bihani et al., 2025).

Beyond the tokenization of physical assets, recent developments highlight the pivotal role of tokens in Decentralized Autonomous Organizations (DAOs). In this model, tokens serve as governance tokens, granting holders voting rights to participate in strategic decision-making regarding protocol Development. This shifts the user-platform dynamic, transforming users from passive consumers into active stakeholders.

Laturnus (2023) posits that tokenization represents a logical evolution, transitioning ownership recording from isolated analog systems to fully integrated digital systems underpinned by cryptographic security and absolute transparency (Laturnus, 2023).

Fundamental Concepts of Decentralisation

Decentralisation in the blockchain ecosystem is not merely the elimination of a central authority; rather, it is a systemic design that distributes functions, control, and trust throughout the entire network. Scientifically defined, decentralisation is a multidimensional variable encompassing technical, economic, and social aspects.

The Decentralisation Trilemma

In the blockchain ecosystem, decentralisation functions as a security architecture. To understand its resilience, it must be viewed as an entity composed of interlocking layers. The discussion is as follows.

Architectural Decentralisation, physical Infrastructure Resilience. Whereas a traditional bank may rely on a single massive data centre, blockchain opts for "antifragility" by distributing its power. Architectural decentralisation answers the question: *How many physical computers comprise this network?* Practical Application, through peer-to-peer (P2P) networks, every node maintains an identical copy of the data. Key Value, elimination of Single Points of Failure. Technically, this system is designed to remain functional even if a significant portion of the hardware is destroyed or forcibly shut down, (Egunjobi et al., 2024).

Political Decentralisation, distribution of power and control a network may possess millions of computers (architecturally), yet if a single corporation owns all those computers, the network remains politically centralised. Political decentralisation addresses the question: *Who controls the hardware?* Practical Application, through consensus mechanisms such as Proof of Stake or DAO governance, decision-making power is distributed among

thousands of distinct individuals. Key Value, resistance to collusion. An ideal system ensures that no small alliance (cartel) can unilaterally alter protocol rules for personal gain, (Ovezik et al., 2025).

Gini Coefficient & HHI (Economic Fairness Indices) These two metrics are adapted from macroeconomics to dissect wealth concentration within the ecosystem. Gini Coefficient, used to assess the inequality of token distribution among asset holders. A score approaching 1 indicates a "Plutocracy," where voting power is dominated by a few wealthy individuals (Whales). Herfindahl-Hirschman Index (HHI), focuses on market concentration. In the context of blockchain, HHI detects whether validation power is accumulating within specific service providers, such as centralized exchanges or large staking pools, (Harang Ju et al., 2024).

Entropy Metrics (System Diversity and Dynamics) Adapted from information theory, this metric measures the level of "uncertainty" or diversity within the network. Core Concept, it quantifies the extent of random and dispersed influence on decision-making. Significance, high entropy indicates that influence is distributed evenly and dynamically. This prevents the system from becoming rigid and complicates attackers' efforts to predict whom to bribe or target to manipulate consensus outcomes, (Anagnostakis & Glavas, 2025).

Blockchan Trilemma

The Blockchain Trilemma is a fundamental concept that describes the structural challenges in developing Distributed Ledger Technology (DLT). This term highlights the inherent difficulty of creating a blockchain network that can simultaneously achieve three primary attributes: Decentralisation, Security, and Scalability.

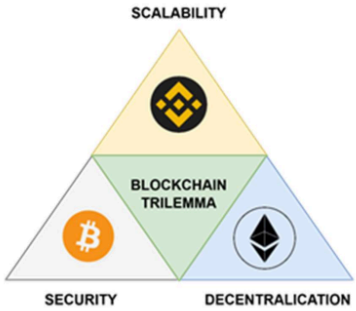

Figure 1. Blockchain Trilemma

This Trilemma is not merely a theoretical construct but a tangible technical hurdle for network architects, underscoring the difficulty of balancing Decentralisation, Security, and Scalability. In practice, developers are often compelled to make trade-offs; they typically must choose two attributes to maximise, while the third is inevitably compromised. For

instance, networks such as Bitcoin and Ethereum (prior to Ethereum 2.0) prioritised high levels of decentralisation and security. However, they faced significant limitations in scalability and transaction processing speed. (Li et al., 2025)

Definitions of the Three Core Pillars

To comprehend the dynamics of this trilemma, clear definitions of each pillar are essential. These three components are described as follows.

Decentralisation, the extent to which control and decision-making within the network are distributed across numerous participants (nodes) rather than being concentrated in a single authority. A greater number of independent nodes participating consensus correlates with a higher degree of decentralisation, implying increased network resistance to censorship. Security The network's ability to maintain data integrity and withstand malicious attacks, such as majority attacks (51% attacks), Sybil attacks, or transaction manipulation. Security relies heavily on robust consensus mechanisms and substantial computational resources for block validation.

Scalability, the network's capacity to accommodate growth in the user base and transaction volume. This is frequently measured by metrics such as Transactions Per Second (TPS) and block finality time. A scalable network must be able to process thousands of transactions rapidly without incurring exorbitant fees, (Khobragade & Turuk, 2023).

Trade-off Dynamics

The relationship between these three pillars is characterized by inherent tension. The study elucidates that within current blockchain protocol infrastructure, there exist efficiency limits that are difficult to transcend. Fundamentally, an inverse relationship exists among these attributes.

Should developers aim to drastically enhance scalability (for instance, by increasing block size or reducing block time to accommodate higher transaction throughput), this necessitates increased hardware and bandwidth requirements for validator nodes. Such elevated requirements make it difficult for ordinary users to operate nodes, resulting in a reduction in the number of validators. This decline in node count directly compromises decentralization.

Conversely, if the focus is placed on maximizing decentralization by involving thousands of geographically distributed nodes, the latency required for data propagation and consensus achievement increases, thereby inhibiting scalability, (Huang & Huang, 2025).

Contemporary Solution Approaches

Recognising that perfectly resolving this trilemma at the base layer (Layer 1) is exceedingly difficult, research during the 2023–2025 period has focused on alternative approaches and layered architectures. Key solutions currently dominating academic discussion include:

Layer-2 Solutions (L2 Rollups): This approach offloads the majority of the computational burden and transaction processing from the main chain (mainnet). Layer-2 processes thousands of transactions off-chain and then aggregates them into a single, concise proof, which is submitted back to Layer-1 for security.

Consensus Mechanism Innovations: Research, such as that discussed in IEEE Access (2024), explores alternative consensus

mechanisms beyond traditional Proof-of-Work (PoW) and Proof-of-Stake (PoS), including Proof-of-Capacity and reputation-based consensus. These innovations aim to balance energy efficiency with the requirements of decentralisation, (Alghamdi et al., 2024).

Current Trends (2024–2025)

In recent literature, the paradigm of blockchain Development has shifted from Monolithic to Modular designs. Decentralization is no longer confined to the base layer (Layer-1). However, it is now implemented using Zero-Knowledge Proofs (ZKP) and the separation of network functions to address the Blockchain Trilemma.

Integration of Zero-Knowledge Proofs (ZKP) for Privacy

ZKP (specifically, zk-SNARKs and zk-STARKs) enables verifying computational integrity without revealing the underlying input data. This is crucial for maintaining blockchain transparency while simultaneously protecting user privacy.

Technically, ZKP reduces the verification burden on Layer-1 nodes; instead of re-executing every transaction, nodes need only validate a succinct cryptographic proof that the computation is correct. This strengthens decentralization by lowering hardware barriers for small validators, (Gupta SATI, 2025).

Layer-2 Scalability and EIP-4844 (Proto-Danksharding)

One of the most significant technical leaps in 2024 was the implementation of EIP-4844 on the Ethereum network. This technology introduced "blobs" (Binary Large Objects) temporary data spaces explicitly designed for Layer-2 Rollups. Theoretically, this separates the Execution Layer (where transactions are processed) from the Data Availability Layer (where transaction data is stored for verification).

Connection to Tokenomics, the reduction in transaction fees by 10 -100x through this mechanism allows utility tokens to be utilized in micro-transactions that were previously economically unfeasible.

Incentives, incentive mechanisms now also encompass "Sequencers" on Layer-2, responsible for ordering transactions, creating new economic dynamics for token holders within the ecosystem, (Qi et al., 2024).

Modular Architecture and Data Availability (DA)

Trends in 2024–2025 indicate that the future of decentralisation relies on layer specialisation. Protocols such as Celestia and Avail provide specialized DA layers, enabling blockchains to no longer need to handle every function on a single chain (a monolithic approach).

This approach allows "App-chains" (application-specific blockchains) to operate on top of existing security infrastructure, expanding the capability of smart contracts to handle millions of users without compromising cryptographic security, (Li et al., 2025).

METHOD

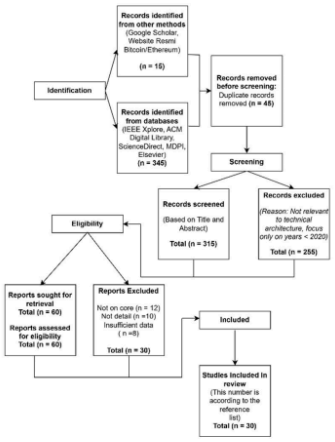

Figure 2. PRISMA Flow Diagram

This section outlines the systematic procedures employed in this study, structured into three primary components: the research design, the population and sample (research targets), and the techniques used for data collection and analysis.

Research Design

This study employs a qualitative descriptive research design utilizing a Systematic Literature Review (SLR) approach. The SLR framework was selected to systematically identify, evaluate, and interpret comprehensive research findings on fundamental blockchain architecture, tokenisation mechanisms, and data decentralisation principles. This design enables a rigorous synthesis of the current literature to address research questions on the comparative analysis of Distributed Ledger Technology (DLT) and conventional databases, as well as their evolving roles as digital trust infrastructures.

Population and Sample (Research Targets)

The population for this study comprises scientific literature sourced from internationally reputable academic databases, specifically IEEE Xplore, ACM Digital Library, ScienceDirect, MDPI, and Elsevier. From this population, the sample (research targets) was selected using a purposive sampling strategy based on strict inclusion and exclusion criteria to ensure data quality and validity, Inclusion Criteria:

Scientific journal articles and reputable international conference proceedings discussing technical aspects, system architecture, and blockchain economic models (tokenomics). Literature published within the last three years (2023–2025) to capture the most recent advancements. Articles presenting comparative data or case studies related to the implementation of decentralization and cryptographic security. Articles written in English.

Exclusion Criteria, Articles focusing solely on market analysis or crypto asset price fluctuations without in-depth technical discussion. Commercial project Whitepapers that have not undergone peer review. Articles that do not provide full-text access or consist only of abstracts.

Data Collection and Data Analysis Techniques

Data Collection Techniques: Data collection was conducted through a systematic search strategy focusing on publications from the last three years (2023–2025) to ensure relevance to highly dynamic developments in blockchain technology, particularly Layer-2 innovations and modern consensus mechanisms. The search strategy employed specific keywords structured using Boolean operators (AND, OR), including: *"Blockchain Architecture", "Consensus Mechanism", "Tokenomics", "Decentralization Metrics", "Distributed Ledger Technology",* and *"Smart Contracts".*

Data Analysis Techniques: The collected data were analyzed using content analysis and comparative methods. The analysis process focused on four primary dimensions: Block working mechanisms and data validation. Security characteristics (immutability and transparency). The role of tokens as incentive instruments. Architectural and political decentralization principles.

Information from the selected sample was synthesized to map the strengths and weaknesses of blockchain technology compared to traditional databases and to identify contemporary solutions to the "Blockchain Trilemma" (Decentralisation, Security, Scalability). The results are presented descriptively and summarised in comparative tables to clarify the fundamental differences between the systems.

RESULTS AND DISCUSSION

Comparative Analysis: Traditional Database Architecture vs. Distributed Ledger Technology

Blockchain has emerged as a disruptive innovation, transforming traditional industrial operations by providing a decentralized system that ensures data security and transparency. The evolution of data management paradigms has reached a crucial transition point, shifting from centralised storage models to decentralised systems.

Fundamental Differences in Architecture and Governance

As delineated in Table 1, the primary distinction lies in the architectural foundation. Traditional databases rely on a Client-Server model in which data is stored on a central server controlled by a single administrator. This structure grants the administrator "Super User" privileges, allowing them full authority to create, modify, or delete data.

In contrast, Blockchain utilizes a Peer-to-Peer (Distributed) architecture. There is no central administrator; instead, validation is conducted collectively by the majority of the network through a decentralized consensus protocol (such as PoW or PoS). Each node possesses a full copy of the ledger, eliminating the reliance on a single central authority.

Data Integrity: Mutability vs. Immutability

A critical finding regarding data management is the contrast between CRUD and Append-Only mechanisms.

Traditional Databases: Operate on CRUD (Create, Read, Update, Delete) principles. Data remains mutable and can be edited or deleted at any time by authorized parties, rendering it vulnerable to internal manipulation.

Blockchain: Enforces an Append-Only structure. Once a block is added, the data becomes permanent and immutable. Security is guaranteed not by perimeter firewalls, but by cryptographic functions (such as SHA-256) and digital signatures. Any attempt to alter a single piece of data would break the hash chain, making the system tamper-evident.

The Trade-off: Efficiency vs. Resilience

The analysis reveals a significant trade-off between operational efficiency and system resilience.

Efficiency: Traditional databases are highly efficient and cost-effective, capable of processing millions of transactions per second (TPS) with low latency. However, they suffer from a Single Point of Failure (SPOF) if the central server is compromised, the entire system collapses.

Resilience: Blockchain offers Fault Tolerance. The system continues to operate normally even if a portion of the nodes is attacked or goes offline. However, this redundancy comes at a cost: the system is computationally intensive and energy-intensive, and it currently faces scalability limits (the Blockchain Trilemma), often requiring Layer-2 solutions for high-volume processing.

Shifting the Trust Paradigm

Ultimately, the transition from traditional databases to Blockchain represents a shift from Institutional Trust (relying on the organization managing the data's reputation) to Code-based Trust (relying on open-source mathematical algorithms). This moves the ecosystem from an "Opaque" state, where auditability is difficult, to a "Transparent" state, where anyone can audit transaction history in real-time via a Block Explorer.

Table 1. Technical Comparison: Traditional Database (Centralized) vs. Blockchain (Decentralized)

Comparison Aspect	Traditional Database (Centralized)	Blockchain (Decentralized)
Network Architecture	**Client-Server** (Centralized storage)	**Peer-to-Peer** (Distributed ledger)
Control Model	**Single Authority** (Admin is *Super User*)	**Decentralized Consensus** (Majority validation)
Data Mutability	**Mutable** (CRUD: Editable & Deletable)	**Immutable** (*Append-Only*: Permanent)
Security Layer	**Perimeter-Based** (Firewalls & Access Logs)	**Cryptographic** (Hash Chains & Signatures)
Transparency	**Opaque** (Closed / Private access)	**Transparent** (Real-time public audit)
Resilience	**Fragile** (*Single Point of Failure*)	**Fault Tolerant** (Resilient to node failure)
Trust Model	**Institutional** (Trust in Intermediaries)	**Trustless** (Trust in Code & Math)
Performance	**High** (High throughput & efficiency)	**Restricted** (Limited by *Trilemma*)
Cost Efficiency	**Efficient** (Low resource redundancy)	**Resource Intensive** (High redundancy cost)

Empirical Validation of Security Limitations in Centralized Systems

The inherent limitations of centralized database architectures are substantiated by

empirical evidence presented by Wintolo, Riadi, and Yudhana (2025) regarding security vulnerabilities within Open Journal Systems (OJS). Their research revealed that systems reliant on a single-server architecture are critically susceptible to Single Points of Failure (SPOF), in which intruders can inject malicious files and manipulate data undetected in the absence of external forensic mechanisms. These findings underscore the fundamental weakness of mutable data integrity in conventional systems, where security is heavily dependent on manual administrator intervention and periodic backups. Consequently, this case study validates the urgent need for a paradigm shift toward a Blockchain architecture, where the characteristics of immutability and decentralization eliminate reliance on a single administrative entity and ensure data integrity through cryptographic network consensus, (Riadi et al., 2021).

The Intersection of Technical Security and Digital Literacy

While blockchain architecture establishes a robust technical foundation for data integrity through cryptographic consensus, the overall security of the ecosystem remains intrinsically linked to the user's capability to manage digital assets. A recent study by Riadi et al. (2025) on digital literacy highlights the critical role of human awareness in mitigating cyber threats such as phishing and malware. Their findings suggest that technical safeguards must be complemented by educational initiatives to enhance user understanding of data protection. This is particularly relevant in the context of blockchain's 'self-sovereign' model, where users bear full responsibility for managing private keys without intermediary oversight. Consequently, the transition to decentralized infrastructures requires not only architectural innovation but also the level of digital literacy advocated by Riadi et al., ensuring that the immutable nature of the ledger is not compromised by social engineering vulnerabilities at the user level, (Riadi et al., 2025).

Operational Efficiency in Centralized Architectures

The comparative analysis of database architectures is further contextualized by recent practical implementations in service industries, such as the web-based booking system developed by Dewi, Hamdan, and Sunardi (2025). Their research demonstrates that for applications requiring high-frequency transactions and real-time scheduling updates, traditional relational databases (such as MySQL) remain the superior choice due to their operational efficiency and low latency. The success of their centralized administration model in managing user schedules validates this study's finding regarding the trade-off between performance and security; specifically, that while blockchain excels in trustless environments, centralized databases are indispensable for ecosystems where performance priority outweighs the need for decentralized consensus, (Dewi et al., 2025).

Strategic Approaches to Network Resilience: Detection vs. Architecture

The critical necessity for robust network resilience is exemplified by Sunardi and Suyahman's (2025) comparative analysis of DDoS attack detection using Machine Learning. Their study highlights the persistent threat of traffic-flooding attacks on conventional network infrastructures, necessitating advanced

detection algorithms like Random Forest to maintain service availability. This aligns directly with the core premise of this dissertation regarding the architectural superiority of decentralized systems. While Sunardi and Suyahman propose a *reactive* software-based solution to identify threats, blockchain technology offers a *proactive* architectural solution by eliminating the Single Point of Failure (SPOF). Thus, the transition to Distributed Ledger Technology (DLT) effectively complements such detection mechanisms by dispersing network data across peers, rendering standard DDoS vectors ineffective against the system's global availability.(Komparasi Prediksi Serangan DDoS Menggunakan Machine Learning, 2025)

Endpoint Vulnerabilities in Web-Based Blockchain Access

The structural integrity of blockchain networks must be contextualized within the broader security landscape of user interfaces, as highlighted by Syukri, Riadi, and Sutikno's (2025) forensic analysis of web browser privacy modes. Their findings reveal that standard privacy features in Web 2.0 interfaces fail to completely prevent data recovery from volatile memory, exposing a critical vulnerability at the user endpoint. This establishes a significant 'last-mile' security challenge for blockchain adoption. At the same time, the distributed ledger itself is cryptographically immutable, while the primary access points such as decentralized applications (dApps) and web-based wallets operate within inherently vulnerable browser environments. Consequently, this study posits that the promise of a 'trustless' infrastructure remains incomplete unless the security of the client-side interface is elevated to match the resilience of the underlying blockchain protocol.(Syukri et al., 2025)

Empirical Evidence of Centralized Vulnerabilities vs. Immutable Architectures

The inherent fragility of centralized data architectures is vividly illustrated by the forensic analysis conducted by Wintolo, Riadi, and Yudhana (2025) on Open Journal Systems (OJS). Their study confirms that systems relying on a single administrative point of control are prone to unauthorized file injection and data manipulation, necessitating complex reactive measures to restore integrity. This empirical evidence directly substantiates the comparative analysis presented in this research, specifically regarding the critical distinction between 'mutable' traditional databases and 'immutable' blockchain ledgers. While Wintolo et al. demonstrate that security in centralized models depends heavily on perimeter defenses and backup recovery, this study argues that blockchain's decentralized, append-only structure offers a superior architectural solution, where data integrity is mathematically guaranteed by consensus rather than susceptible to administrative compromise, (Wintolo et al., 2025).

Algorithmic Objectivity in Centralized vs. Decentralized Architectures

The growing reliance on algorithmic objectivity to mitigate human bias is exemplified by Sunardi's (2025) implementation of the K-Nearest Neighbors (KNN) algorithm for personnel selection. While their web-based solution successfully demonstrates how computational logic can enhance transparency in decision-making, it operates within a traditional, centralized

architecture in which data integrity ultimately rests on administrative authority. This case study serves as a critical reference point for the comparative analysis in this dissertation; it illustrates that while centralized databases (such as those used in Django frameworks) excel in computational efficiency for specific organizational tasks, they lack the tamper-proof guarantees of blockchain technology. Consequently, the transition to decentralized ledgers represents the necessary evolution for ecosystems that require not just algorithmic fairness but also immutable proof of decision-making history, (Sunardi, 2025).

Decentralized Guardianship of Biometric Data in Immersive Environments

The advancement of immersive technologies, as detailed in the review by Rakhmadi, Yudhana, and Sunardi (2024) on Virtual and Augmented Reality for Sign Language Recognition, underscores the massive influx of sensitive biometric data required for accurate gesture processing. While their research addresses the critical need for inclusive human-computer interaction, storing such intimate behavioral data in centralized servers introduces significant privacy vulnerabilities. This context validates the architectural proposition of this study regarding blockchain's role in data sovereignty; specifically, integrating Distributed Ledger Technology (DLT) can transform how these immersive systems manage identity. By replacing centralized data repositories with decentralized identifiers (DIDs), blockchain ensures that the biometric inputs captured by VR/AR interfaces remain under the user's cryptographic control, thereby solving the privacy paradox inherent in the adoption of the Metaverse and advanced recognition systems, (Rakhmadi et al., 2024).

Network Privacy Paradox: Algorithmic Classification vs. Cryptographic Pseudonymity

The challenge of balancing user privacy with verifiable identification within network infrastructures is rigorously analyzed by Riadi, Fadlil, and Prabowo (2024). Their research on MAC address randomization demonstrates that, in centralized systems, enhancing privacy often compromises administrative visibility, necessitating complex machine learning solutions such as Gaussian Naïve Bayes to classify user identities. This dichotomy serves as a critical baseline for evaluating blockchain architecture; unlike centralized networks that struggle to manage randomized hardware identifiers, blockchain solves the privacy-transparency paradox through cryptographic pseudonymity. By abstracting identity from device-specific MAC addresses to public keys, decentralized ledgers provide a structural solution that preserves user anonymity without sacrificing the network's ability to validate transactions, effectively superseding the need for probabilistic classification methods in traditional network management, (Riadi et al., 2024).

Data Integrity Foundations for AI-Driven Critical Systems

The deployment of deep learning models for high-stakes decision-making, as demonstrated by Sunardi et al. in their application of Convolutional Neural Networks (CNNs) to flight route optimization, underscores the pivotal reliance on the reliability of input data. While their research successfully addresses the computational

challenge of dynamic routing based on weather conditions, the system inherently assumes that these input variables remain uncorrupted by malicious interference or centralized transmission errors. This scenario validates the dissertation's architectural proposition that immutable data layers are necessary. By integrating blockchain technology as the foundational trust infrastructure, the integrity of environmental data fed into such CNN models can be cryptographically guaranteed, ensuring that sophisticated optimization logic acts upon verifiable truths rather than potentially manipulated centralized datasets, (Sunardi et al., 2024).

CONCLUSION

This study concludes that blockchain technology represents a fundamental architectural shift from centralized, administrator-dependent systems to decentralized, cryptographic trust infrastructures. The comparative analysis reveals that while traditional relational databases (utilizing the CRUD model) offer superior performance in terms of throughput and latency for general-purpose applications, blockchain's distributed append-only ledger structure provides unmatched advantages in data integrity, immutability, and censorship resistance. Furthermore, the synthesis of recent technical literature (2023–2025) highlights that the "Blockchain Trilemma" the historical trade-off between scalability, security, and decentralization is being effectively addressed through the transition from monolithic architectures to modular Layer-2 systems, specifically through the implementation of Optimistic Rollups and Zero-Knowledge Proofs. Additionally, the Nakamoto Coefficient has proven a critical metric for evaluating the resilience of these networks against collusion and single points of failure.

Based on these findings, this research offers several recommendations and directions for future work. First, organizations should view blockchain not as an absolute replacement for conventional databases, but as a specialized solution for ecosystems that require high transparency and "trustless" interactions without a central authority. Second, regarding limitations, this study primarily employed a qualitative Systematic Literature Review (SLR) approach; therefore, future research should focus on quantitative benchmarking to empirically measure the transaction throughput (TPS) and latency differences between Layer-1 and Layer-2 solutions under stress-test conditions. Finally, further investigation is recommended into the interoperability standards between heterogeneous blockchain networks and the integration of quantum-resistant cryptography to ensure the long-term security of digital assets and tokenized ecosystems.

REFERENCE

1_similarity 94 Sumarhadi

ORIGINALITY REPORT

3%	2%	2%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Amit Kumar Tyagi. "Next Generation Blockchain for Next Generation Society with Futuristic Technologies", CRC Press, 2026 Publication	1%
2	yodaplus.com Internet Source	<1%
3	Submitted to Middlesex University Student Paper	<1%
4	Rishabha Malviya, Sonali Sundram. "Blockchain for Healthcare 4.0 - Technology, Challenges, and Applications", CRC Press, 2023 Publication	<1%
5	www.ifcreview.com Internet Source	<1%
6	Jamuna S. Murthy, G. M. Siddesh, K. G. Srinivasa. "Cloud Security - Concepts, Applications and Practices", CRC Press, 2024 Publication	<1%
7	www.aijmr.com Internet Source	<1%
8	www.fastercapital.com Internet Source	<1%
9	files.eric.ed.gov Internet Source	<1%

10	journals.sagepub.com Internet Source	<1 %
11	jmi.rivierapublishing.id Internet Source	<1 %
12	jpmi.journals.id Internet Source	<1 %
13	www.amongtech.com Internet Source	<1 %
14	fastercapital.com Internet Source	<1 %
15	"Cryptology and Network Security with Machine Learning", Springer Science and Business Media LLC, 2024 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		