ISSN (Online): Applied
International Journal of Engineering, Technology and Computer Science
Vol. 1 | Issue 1 | October - December 2025
Available online at: https://ijetcs.com

Blockchain-Based Authentication and Data Integrity Frameworks

Shubham Sharma
Assistant Professor, Department of Computer Application
Shri Lal Bahadur Shastri Degree College Gonda
Er. Abhay Dwivedi
Assistant Professor, Department of Computer Application
Shri Lal Bahadur Shastri Degree College Gonda

Corresponding Author Email Id: abhaydwivedignd@gmail.com

ABSTRACT:

The rapid digital transformation across communication ecosystems has intensified the need for secure, transparent, and tamper-resistant authentication mechanisms. Traditional centralized authentication systems often face vulnerabilities such as single points of failure, data manipulation, and unauthorized access. In response, blockchain technology has emerged as a decentralized and immutable solution capable of strengthening data integrity and trust within digital networks. This research paper explores blockchain-based authentication and data integrity frameworks, emphasizing their structural components, operational mechanisms, and potential applications across diverse domains. By analyzing consensus protocols, cryptographic hashing, distributed ledgers, and smart contract–driven validation processes, the study evaluates the comparative effectiveness of blockchain in contrast to conventional security models. It also highlights the suitability of blockchain for identity management, access control, supply chain validation, academic certificate verification, healthcare records, and secure governmental data systems. Furthermore, the paper investigates key challenges involving scalability limitations, interoperability gaps, resource consumption, regulatory uncertainties, and user-level awareness. The study concludes that while blockchain presents a transformative foundation for secure authentication and data integrity, its widespread adoption requires hybrid architectures, policy-level standardization, and enhanced user literacy. This work contributes to ongoing academic discussions by presenting a theoretical, multidisciplinary perspective on the future of blockchain-enabled security infrastructures.

Keywords: Blockchain; Authentication; Data Integrity; Decentralization; Cryptographic Hashing; Consensus Mechanisms; Smart Contracts; Identity Management.

1. Introduction

Blockchain technology enables new paradigms for authentication and data integrity. To date, most scholarly discourse has focused on the financial sector, neglecting other domains where blockchain principles could improve security. This comprehensive survey identifies four fundamental observer-only properties for architecting blockchain-based, security-oriented frameworks: (1) immutability guarantees; (2) cryptographically verifiable control of assets; (3) specification of globally persistent observation conditions and permission configurations for chosen observers; and (4) decoupling of authentication and data infrastructure control. The paper collects relevant literature from business, health care, identity management, and supply-chain sectors to analyze which blockchain-based security dimensions have received attention, where security gaps remain, and how diverse goals and challenges can be formulated over the four core properties. Gaps may indicate new research avenues, while similarities may yield generic models across disciplines.

2. Foundations of Blockchain Technology

The previous works in the domain elaborated several advantages blockchain technology brings on integrity assurance in the data life-cycle. While this technology can provide non-repudiation, certificates, watermarking, content-based hashing, and other supplementary solutions remain necessary (Zolanvari et al., 2018). In conjunction with the authentication matter, it is vital to properly address the security needs linked to the architecture and governmental topology of such a blockchain. First off, the type of blockchain to implement is crucial. The adoption of permissioned or private blockchains tends to be driven by regulatory or confidentiality reasons, therefore an assessment of the respective rights and responsibilities possessed by the actor in the system must be conducted.

This framework investigates the concept of a public blockchain requiring no log-off and the offer of services on a permissioned basis through actors and certificates. Both security and performance guarantees are largely postulated on the absence of a public chain. Performance bottlenecks and issues impendency arise between state access, completeness, state commitment, and no-roll-back requite a smaller solution space. The ongoing verification only produces pro-gress votes in a precise concurrent manner. A designation with state completion, triggering external acts, while committing weights needs to permit all-inclusive state delivery. Logistic trade-offs arrive with fault tolerance, communication volume, adversary and failure assumption, throughput and bandwidth, resource sharing, and solvers to fix dependencies or state on a desire of lower dynamic $\|DS\|$.

2.1. Distributed Ledger Concepts

Blockchain technology brings a paradigm shift in managing digital information with a distributed ledger (DL) that addresses historical issues of trust among network participants. A DL maintains a consistent state of digital events, known as transactions, that occur across a network of participants. Each transaction recorded in a DL creates a persistent and immutable event that prevents tampering after it is committed. Furthermore, the entire transaction history remains incorruptible and audit-ready because the data structure and transaction validation mechanisms are tamper-evident.

DLs are classified as public, private, or consortium depending on the accessibility of the blockchain management processor (Zolanvari et al., 2018) (Zolanvari et al., 2018). In an open and accessible public DL, all participants retain comparable levels of authority and power over actions taken on the DL; in contrast only approved members can access and participate in activities. Prior to any information being committed, the event is gathered into a block that is subsequently appended to the existing chain of blocks, thereby preserving temporal ordering. This ordering of transactions between the events linked in the chain is conducted via a defined ordering sequence, confirming the event to follow specific rules for consistency throughout the interactions across the DL.

2.2. Consensus Mechanisms

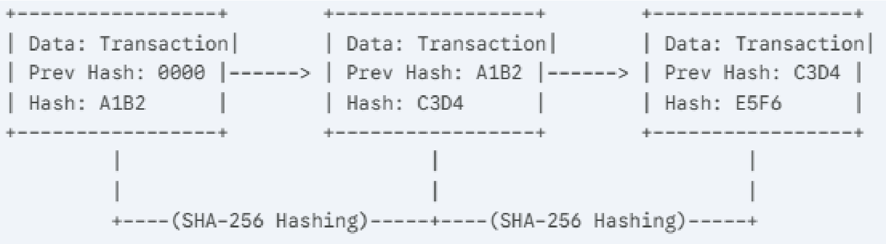
Blockchain is a distributed database that offers tamper-resistant public records maintained by a community of network participants. In a blockchain, data is grouped in blocks linked via hashing to a chain; each block contains transactions appended by participants. To ensure integrity and build trust, system-wide policies determine the conditions for adding blocks.

Consensus mechanisms secure the synchronization of distributed ledgers. These protocols determine the validity of proposed additions and coordinate agreement when they contain conflicting or overlapping information (Yao et al., 2021). Bitcoin introduced proof-of-work (PoW) and established first-mover advantage. Under PoW, consensus is reached through computationally expensive algorithms that require large-scale energy expenditure to provide assurance against sabotage by self-interested parties. For additional security, mechanism-specific efficacy analysis is necessary since the energy–fault tolerance relationship varies widely between consensus types (Zhang et al., 2022).

2.3. Cryptography in Blockchain

Cryptography protects sensitive information and provides three security guarantees needed in a blockchain: data integrity, sender authentication, and non-repudiation. Hash functions, digital signatures, and zero-knowledge proofs play important roles in various blockchains.

A hash function is a widely used mathematical function that takes input data as a string of any length and produces a fixed-length output string, called a hash.



```
+-----------------+        +-----------------+        +-----------------+
| Data: Transaction|       | Data: Transaction|       | Data: Transaction|
| Prev Hash: 0000 |------> | Prev Hash: A1B2 |------> | Prev Hash: C3D4 |
| Hash: A1B2      |        | Hash: C3D4      |        | Hash: E5F6      |
+-----------------+        +-----------------+        +-----------------+
         |                          |                          |
         |                          |                          |
         +----(SHA-256 Hashing)-----+----(SHA-256 Hashing)-----+
```

Figure 1: Illustration of Blockchain Hashing and Block Chaining Mechanism

The same input will always result in the same output since hash functions are deterministic. Four security characteristics are required for a cryptographic hash function: 1) a message with a certain hash value cannot be found (pre-image resistance); 2) two distinct messages with the same hash value cannot be found (second pre-image resistance); 3) a little change in the input must result in a huge change in the output (avalanche effect); and 4) it is infeasible to produce a hash value without seeing the message (collision resistance). While all four properties may not be necessary, the acceptance of a certain hashing algorithm depends on its combination. Since data in blockchain transactions originate from multiple sources and are aggregated into a single block, transaction information cannot be authenticated, yet the identity of the sender needs to be secured in the transaction data. This can be achieved by digital signatures and hash functions. Signing the hash of the message instead of the message itself can provide the same assurance and reduce the workload. Zero-knowledge proof techniques can allow one party to prove possession of sensitive information without revealing the information itself. Thus, an identifier and secret maintain an association while the secret remains undisclosed. Blockchains can be viewed as a secure distributed ledger technology where information is recorded in a chronological manner, and a variety of services (transfer of assets, exchanges of contracts, and more) could be established. Information integrity depends on maintaining data consistently. Consequently, the hash of the information rather than the information itself is stored on the ledger to ensure integrity (Zolanvari et al., 2018).

3. Authentication Paradigms in Blockchain Environments

Users interacting with decentralized applications (DApps) typically connect through credentials and access tokens to access off-chain resources or steer on-chain transactions. Robust access control mechanisms are essential to manage permissions for personal data access and DApp operations. Compared to single instances, a single access right may be assigned to multiple DApps.

Exploiting blockchain for access control necessitates mechanisms to manage these permissions, requiring an approach tailored for its decentralized architecture. Existing frameworks, while suitable for distributed architectures, fall short: blockchain systems warrant the development of dedicated models. The literature outlines three principal paradigms defined by the access right modeling approach (Zolanvari et al., 2018).

3.1. Identity Representation and Decentralized Identifiers

Identity fuels social interaction, facilitating appointments, business transactions, information exchange, and travel. Human communication depends on knowing identities, yet Society 5.0 extends the Internet of Things beyond seamless connectivity to permit interaction among materials, products, services, devices, and people. Industrial and altruistic perspectives converge with economics to engender common notions of authenticity, integrity, and trust, forming the basis for reassuring the various parties involved in identity-related matters.

Building trust and confidence leads to acceptance and co-creation of the social phenomena Society 5.0 seeks to engender. Conventional identity methods prove inadequate for enabling digital authenticity, integrity, and trust via decentralization. Society 5.0 requires a new identification framework with associated address, signature, and time-stamp methods that establish and express uniqueness, authenticity, and integrity throughout interaction processes, supported through an identity-free paradigm-based account for decentralized identity.

Decentralized identity searches for a digital-society address-and-signature method that guarantees authenticity, integrity, and non-repudiation without requiring a pre-existing identity. Profile data erasing and resending maintain confidentiality in a digital society where identity is represented only through the identification process itself. Unlike conventional identity-attached profiles where attributes become observable and usable for abuse, digital-society Personal Unique Identifiers (PUIs) overcome this pitfall where decentralized identity authenticates the interaction without conveying identity (Gilda et al., 2022).

3.2. Access Control Models for Distributed Systems

Access control is a critical security mechanism in traditional systems, regulating the accessibility of resources such as files, data, documents, and devices. These systems employ various methods for controlling access, with RBAC being one of the most widely adopted approaches. However, traditional access control systems depend on a centralized entity to store data and enforce security policies, leading to issues of trust. Various authorization models based on blockchain technology have been proposed to address these concerns (Jodeiri Akbarfam et al., 2023).

Access control serves as a vital security mechanism within conventional systems, governing access to resources such as files, data, documents, and devices. These systems apply diverse methods to control access, with role-based access control (RBAC) being one of the most widely implemented approaches. Nevertheless, traditional access control frameworks rely on a centralized entity to store data and enforce security policies, thereby undermining trust. Several authorization models grounded in blockchain technology have been introduced to mitigate such concerns.

Three fundamental models for access control in distributed systems can be identified: (1) Role-Based Access Control, (2) Attribute-Based Access Control, and (3) Capability-Based Access Control. Within the RBAC model, a role is established for each user profile. By associating permissions with these roles, it becomes possible to control access according to the types of activities assigned to each role rather than to distinct users. The attributes associated with individuals govern permissions and access rights within the ABAC model. Based on access rights and behavior histories, authorization requests are determined by rules specified within the clauses. This model offers swift support for a broad spectrum of authorization requests and facilitates the integration of access control into implementation levels. Whereas the foregoing two models necessitate a third-party entity to enforce control, the capability approach relies on a capability method for authorization, obviating the need for a separate system (Rouhani et al., 2020).

Table 1: Comparison of Access Control Models in Distributed Systems

Model Name	Mechanism	Dependency	Pros & Cons
RBAC (Role-Based Access Control)	Each user is assigned one or more roles; permissions are linked to roles instead of individual users.	Role	**Pros:** Simple to administer and align with organizational job functions. **Cons:** Role explosion and rigid structures can make fine-grained control hard.
ABAC (Attribute-Based Access Control)	Authorization decisions use attributes about users, resources, actions, and context with policy rules.	Attributes	**Pros:** Very flexible and expressive for complex, context-aware policies. **Cons:** Policy design and attribute management can be complex.
CAPBAC (Capability-Based Access Control)	Users receive unforgeable capability tokens that directly encode the rights to access specific resources.	Capability / Token	**Pros:** Decentralized; easy delegation by passing capabilities. **Cons:** Revocation and tracking distributed capabilities can be challenging.

3.3. Reputation and Credentials on Chain

Blockchain technology enables decentralization and trust among unacquainted entities, serving as a natural foundation for attestation systems. Attestations by credential providers affirm identity, reputation, and other attributes, allowing trust to evolve with the use of services (Baldi et al., 2019). In these frameworks, the user-centric model necessitates preventively countering Sybil attacks, wherein users artificially inflate their trust score by creating multiple identities. Various designs exist for limiting the degree of trust that each user can confer, but each carries trade-offs regarding usability and effectiveness. Users maintain the fundamental right to rely on others; nevertheless, Sybil resistance remains a critical consideration in evaluating these architectures.

Trust credentials may depend on technical aspects of blockchain systems. Appendix H enumerates selected facilitating factors along with proactive and reactive Sybil-resistant designs, focusing on those that enhance the user-centric approach. Influencing these factors often incurs design trade-offs elsewhere in the system. Establishing credential systems compatible with prevailing blockchain solutions aids adoption by communities already utilizing them, while secure on-chain credential attestation and custodianship protocols bolster infrastructure governance.

4. Data Integrity Mechanisms Leveraged by Blockchain

The core principle underlying blockchain technology is immutability, which ensures that once data is written to a blockchain, it cannot be changed, thereby establishing a reliable data integrity mechanism. Three primary components contribute to data integrity: (1) immutability, (2) versioning and audit trails, and (3) data provenance and lineage. All three strongly relate to decentralization, data integrity, security, and privacy.

Immutability is inherently present in blockchain-based architectures. When using a distributed ledger, all participants have constant access to the current view of the system, and every transaction is linked to the previous one. Blockchain ledgers are thus append-only, and tampering with any part of the chain is easily detectable (Zolanvari et al., 2018). These structures are pervasive, and many mechanisms exist to harden them against undesired changes. The evolution of the blockchain is always traceable, allowing extensive auditing of the system from its origin. In practice, ledgers permit inserts and updates, while deletes are rare. Snapshots of the current state can therefore be taken periodically to limit growth; subsequent evaluations can then treat the log as a set of events which can often be managed more compactly.

4.1. Immutability and Tamper-Evidence

Blockchain ensures data immutability and tamper-evidence by preventing modifications once recorded in a transaction, thus maintaining data integrity and security through cryptographic techniques (Jodeiri Akbarfam et al., 2023). A transparent and high accountability transaction record linked to users enhances trust and collaboration without requiring a central authority. Security measures to safeguard such integrity include user registration with key pairs to prevent unauthorized access, cryptographic signatures to detect tampering, nonces to thwart replay attacks, encryption to guard against man-in-the-middle attacks, role-based permissions restricting subsequent stage changes, token-based encrypted data storage, and blockchain logging for auditing and detecting malicious activity.

Privacy regulations, such as General Data Protection Regulation (GDPR) requests for the right to be forgotten, challenge the immutability of such a system. Forensic audits to retrieve the original entry are permitted; however, complete removals would compromise trust. Similarly, illegal material must be deleted if initially stored, yet the requirement remains for preserving original content securely to avoid integrity violation. Greater flexibility is thus required to accommodate verifiable mutability on blockchain systems (Daniel & Tschorsch, 2021).

4.2. Versioning and Audit Trails

Due to the append-only nature of blockchains, the users of a shared database also remain the exclusive and trustworthy controllers of the data, thereby giving them the right to modify as well as to eliminate the user-unfriendly and even dumped data automatically to preserve free space (Carlos López-Pimentel et al., 2021). One reasonable arrangement in many situations is to permit changes to the recorded data but imposing the same condition that nothing can be removed. Consequently, it is still possible to track the evolution and lots of kinds of data such as log files and values of sensor in such systems. Time goes on and requirements materially grow in many domains like value-transfers, record keeping, customer satisfaction, etc. Non-relational shared data are gaining momentum in the area of event-historized monitoring as storing such lengthy and selective history on-chain is generally too costly (Jodeiri Akbarfam et al., 2023). In such cases to record such versioned full logs, event logging and retention tend to be performed in non-blockchains and a cryptographic backward-linking to only some selected stages is offered by chains.

4.3. Data Provenance and Lineage

Blockchain technology can enhance data provenance and lineage to guarantee data integrity. This approach uses the blockchain itself as a logging mechanism to monitor operations performed on data items belonging to a specific data producer. Data provenance is defined as “the description of the origins and history of an object” (Ramachandran & Murat Kantarcioglu, 2017) , while lineage describes the origin and subsequent transformations that an object underwent (Jodeiri Akbarfam et al., 2023). Data objects logged on the blockchain allow traceability along the service chain, indicating that every service involved in the processing of the data belongs to the original data producer and the modifications are accepted.

Moreover, data can be sent in range-encrypted format along the service chain, enabling the producer to be assured that all operations performed on its data are legitimate and in line with the service agreement. By combining these two pieces of information—traceability and range-encryption—end-to-end integrity can be achieved, thus significantly improving data assurance and consumer confidence.

5. Architectures for Blockchain-Based Authentication and Integrity

The choice between public and permissioned blockchain affects governance, throughput, confidentiality, and trust assumptions. Public blockchains support a wide range of participants but are limited to asynchronous consensus protocols such as Proof of Work (PoW) or Proof of Stake (PoS), which may delay transactions, compromise data confidentiality, and provide no granularity for regulatory compliance (Zolanvari et al., 2018). Permissioned blockchains allow the selection of nodes capable of writing to the ledger, enable higher throughput, accommodate asynchronous and Byzantine fault-tolerant protocols, and improve data confidentiality. Nonetheless, these systems use a central authority to define the initial network and maintain governance; without a universally trusted body, public consensus algorithms are often implemented through smart contracts (Newell et al., 2021).

Hybrid and layered architectures seek to combine the advantages of various blockchain types, yet trade-offs among security, trust, and efficiency are unavoidable. Layer-2 solutions (state channels, payment networks, sidechains) augment scalability and throughput for Bitcoin and Ethereum, whereas sidechains are capable of larger, more diverse extensions within the same family. Overlay solutions do not resolve interoperability challenges between distinct public blockchains.

5.1. Public versus Permissioned Blockchains

Public and permissioned blockchains constitute a continuum of choices encompassing three important dimensions: architecture, level of decentralization, and scope of trust (Truong et al., 2019). While any blockchain arrangement can be fully decentralized, scalability, privacy, and governance—especially within enterprises—can prompt restrictions.

Table 2: Comparison of Public and Permissioned/Private Blockchain Architectures

Feature	Public Blockchain	Permissioned / Private Blockchain
Accessibility	Open for anyone to read, write, and validate transactions; all nodes have similar authority.	Participation limited to approved members; access and actions controlled by policies.
Governance	Fully decentralized; no single trusted administrator or owner of the network.	One organization or a consortium defines membership rules and maintains governance.
Performance	Lower throughput and higher latency because of heavy consensus (e.g., PoW/PoS).	Higher throughput and faster confirmation times due to lighter, coordinated consensus.
Confidentiality	Transaction data is broadly visible, which can reduce confidentiality.	Data visibility can be restricted to specific parties, improving confidentiality.
Consensus Mechanisms	Commonly uses open, permissionless protocols such as PoW or PoS.	Often uses Byzantine fault-tolerant or voting-based protocols tailored to members.
Regulatory Compliance	Harder to align with strict regulatory or KYC/AML requirements.	Easier to integrate identity, audit, and compliance controls for regulated environments.
Typical Examples	Bitcoin, Ethereum (mainnet).	Hyperledger Fabric, R3 Corda, Quorum.

Accordingly, some implementations adopt a more restrictive setup known as a permissioned or private blockchain, in which authorization regimes govern who can join the network, read the ledger, submit transactions, or currently, execute smart contracts. Popular platforms include Hyperledger Fabric and Corda. Other networks support only certain permissions; they distinguish among open public decentralized, partly private, and permissioned arrangements (Gilda et al., 2022).

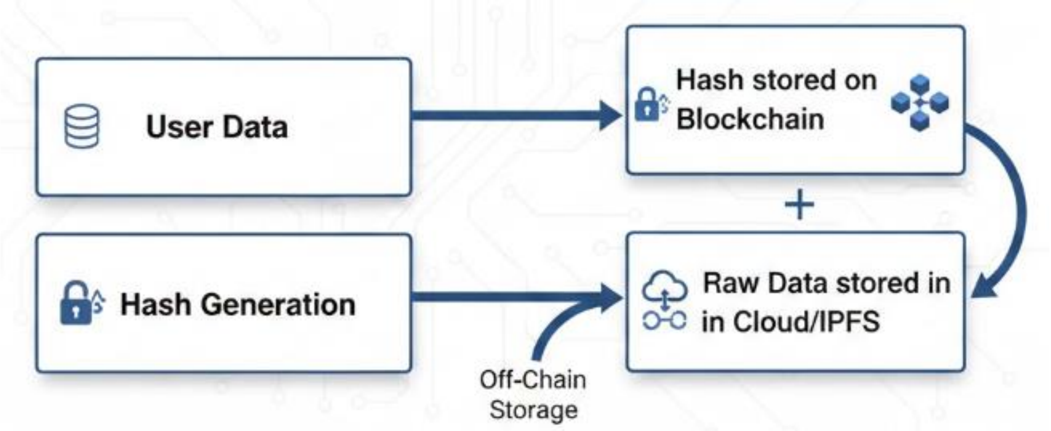
Purely public or private solutions exist as extreme cases along a continuum. As earlier assertions about centralization affirm, partially decentralized solutions exist. Well-known examples include, respectively, Borderless Bitcoin with total control and Sociocracy with approval on every transaction, among others.

5.2. Hybrid and Layered Solutions

Layer-2 and sidechain solutions extend a blockchain's scalability and user privacy. A layer-2 network processes transactions off the main chain while preserving its security. Sidechains operate outside the primary blockchain, permitting different security and privacy levels. Hybrid architectures also combine blockchain solutions with distinct data storage and processing systems but still maintain anchor services for data integrity (Gilda et al., 2022). A layered protocol must support other blockchains for authenticating and verifying.

5.3. Off-Chain Data and On-Chain Anchoring

Once a data element is stored on a blockchain, its origin can no longer be altered. The original data must first be digitally signed before being saved. The signature is hashed before storage, producing a small record in the blockchain. Signing ensures that provenance declaration cannot be denied. As the capability to backtrack provenance further increases the amount of information appended to an object, a hash of the entire provenance record can be added when the stored state reaches a certain amount. In each case an off-line model can be used. The system automatically generates a certificate that includes the data information, content, signature, and the associated hash of the last provenance. The execution logs are recorded onto a lightweight blockchain layer and are referenced within the main blockchain ledger. Any time a smart contract interacts with it, only the complementary information, namely the hash of the last provenance and the certificate, need to be further filled in in the uptaking process. Consequently, the off-line capability set is protected while maintaining the integrity of the origin, provenance, and all through the restricted air-gapped. Heterogeneous distributed environments composed of different cloud platform and blockchain infrastructure are supported at the same time (Liu et al., 2021).



The increasing attention paid to the provenance problem has created new opportunities for blockchain technology. The origin and provenance information of data has attracted importance from the users. Researchers investigate technology to verifiably track the original of data in large-scale cloud systems. The upstream authority creates a source data and then a trusted watermark is inserted in the data. The utilization and verifiability of incoming data undergo strict model evidence with the off-line backtracking (Jodeiri Akbarfam et al., 2023).

6. Evaluation Frameworks and Metrics

Security and integrity metrics determine the assurance that an authentication or data storage scheme can provide. An evaluation framework for security and integrity in authentication systems may incorporate, for example, the assurance level associated with the user authentication process; the exposure risk linked to the credentials stored in authentication systems; and the propagative time needed to verify the correctness of the user credential provided by the requester (Zolanvari et al., 2018). Blockchain-based solutions may also be compared with traditional approaches, and the security areas of authentication, data privacy, data integrity, and data confidentiality may be analysed to give a broader understanding of the risk exposure of the respective solutions.

Performance and scalability metrics characterise the power of a scheme to operate with a high throughput of operations, short latency in the execution of operations, low resource requirements, and a minor cost per transaction. An authentication system, for instance, can be assessed by measuring the amount of time needed to authenticate a user, how much input or output of resources it requires per authentication, and how much monetary cost it entails, depending on the ledger employed or the communication mechanisms adopted. Data storage solutions are evaluated according to the updating time necessary for storing a new data block, the amount of time spent to retrieve a historical data block, the resource usage, and the cost of managing data blocks, which depend on the size of the stored data, the blocking mechanism, or the additional communications for recovery purposes (Zhang et al., 2019).

Metric Category	**Parameters**
Security	Tamper-resistance, data integrity, immutable logging
Performance	Throughput (TPS), latency, resource utilization
Economic Efficiency	Cost (gas fees, storage costs), deployment and maintenance overhead
Interoperability	System compatibility, cross-chain communication and integration capabilities

6.1. Security and Integrity Metrics

The security and integrity of data in a blockchain-based architecture can be assessed through well-defined and structured metrics. Security metrics measure the level of assurance that an asset is not exposed to threats, whereas integrity metrics quantify the degree to which the asset remains unchanged throughout its lifecycle. Three particular dimensions can be considered to address the assurance of security: assurance levels—defined by security properties such as confidentiality, integrity, authentication, availability, and reliability—the avenues of threat exposure; and the latency of verification, which distinguishes the time required to ascertain that data is still valid and without alteration through an established model of assurance level or metric of integrity. Integrity metrics can comprise the number of entities altering data; the proportion of data altered versus unaltered; and the overall number of modifications, which can be distinguished by granularity level.

6.2. Performance and Scalability Metrics

Performance and Scalability Metrics. High system throughput enables it to support a large number of users and a high rate of legitimate transactions. The scalability and performance of the framework are evaluated in terms of transaction execution time, the delay time of the last block, the time delay of the last transaction, energy expenditure, and resource utilization. Keeping the number of edges and user authenticated to the framework, the delay of the last block increases with the increasing number of IoT end points in other frameworks. The average transaction throughput remains stable with a moderate drop because the number of nodes participating in the transaction affects the verification time of the blockchain-based framework. High system throughput enables high rates of legitimate transactions and a large number of users. Performance evaluation demonstrates that the proposed framework, 27.94% greater throughput than benchmark approaches for large-scale transactions. During batch authentication, costs are also reduced 75.61% compared to existing solutions. The performance of the proposed architecture is evaluated in terms of the authentication delay, the average number of transactions in block, and the average batch time. Performance evaluation is based on average end-to-end delay from the edge to cloud as 46.3 ms, average jitter as 2.2 ms, and average packetdrop is 2%. The processing time and cost of an intelligent node rises with the increasing number edge nodes.

Throughput is defined as the number of processed transactions per second, while latency indicates the time from transaction submission to block mining. Resource utilization is quantified through the total usage of CPU, memory, disk, and network while speed monitoring involves transmitting a constant size message. The performance analysis measures the resource consumption, execution time, and latency of the proposed blockchain framework. An authentication mechanism reduces ethe costs. On the ethereum public blockchain, the registration time of a single user only takes 224.72 ms, and 172.74 ms is required for the authentication of one user. The proposed system is tested on the Ethereum testnet using the Gorli test chain, where blocks are generated every 2–3 min. Multiple users from 1 to 20 are registered to analyze the relationship among message size, execution time, and ether cost. Moreover, performance has been tested on Ethereum simulated environment. The run time is reduced and little ether is consumed for additional user registrations with the increase in the maximum number of concurrent requests. Increase in concurrent requests suggests that performance improves across the board, with reduced time and cost for each additional user who logs into the system (Umoren et al., 2022).

6.3. Adoption and Interoperability Metrics

Adoption and interoperability metrics help assess the standing of blockchain solutions on the innovation spectrum. Blockchain adoption indicates the extent of various human activities and the number of entities participating under a blockchain architecture. The definition of blockchain, entities and activities remain ambiguous across the literature. First, a broad and comprehensive exploration of blockchain definitions and implementations provides insights on what constitutes blockchain adoption today. Second, a typology of the blockchain ecosystem with a focus on blockchain activities and roles within a purpose-oriented perspective (Gilda et al., 2022) helps ascertain what the term adoption entails at a grand scale. Building on these preliminary results, the levels of adoption for an individual blockchain framework can be evaluated along each dimension of the typology.

Interoperability metrics concern the need for multiple blockchains to co-exist and interoperate within a broader framework. Interoperability relates the capacity of diverse blockchain solutions to communicate, share data transactions and assets, and trigger events across technologies and protocols. Mutual interaction between blockchains can occur either passively or actively, with the former enabling a state of co-evolution. Interoperability characterizes the mass adoption of blockchain platforms, as companies prefer to extend an existing environment rather than undertake the costs and risks associated with a separate infrastructure (Kang et al., 2022). The state of blockchain interoperability goes beyond industry-specific and technology-specific interoperability, since the architecture encompasses extant and emergent standards that are independent from the individual blockchain platforms themselves. Solutions and paths towards greater interoperability can thus be evaluated, along with remarks on the design and architectural choices involved.

7. Challenges, Limitations, and Research Gaps

Over the years, several OSN vulnerabilities have been reported, including information retention, account impersonation, unauthorized data sharing, and identity theft. Such challenges stem from users neither being aware of the rights granted to respected third parties nor having control over the collected data. The pressing concern about OSNs boils down to users being unable to manage their digital identity.

Challenge Category	Key Issue	Description / Impact
Technical	Scalability	Network performance can degrade as the number of transactions and participating nodes increases.
Technical	Interoperability	Exchanging data and assets across heterogeneous blockchain platforms and legacy systems is difficult.
Technical	Storage Overhead	The continuously growing ledger size creates long-term storage and

Challenge Category	Key Issue	Description / Impact
		synchronization challenges.
Regulatory	GDPR Compliance	Tension exists between immutable records and requirements such as the “right to be forgotten”.
Regulatory	Legal Framework	Many jurisdictions lack clear rules for smart contracts and decentralized digital assets.
Social	User Awareness	Limited understanding of keys, wallets, and security practices leads to misuse and vulnerabilities.
Social	Adoption Resistance	Institutions may hesitate to migrate from familiar centralized models to decentralized solutions.

Self-sovereign identity (SSI) (Zolanvari et al., 2018) enables individuals to manage their digital identities without relying on any third party. SSI operates on blockchain technology, which offers sufficient protection against unwanted attacks. Blockchain-based solutions such as blockcerts, credchain, and datacert allow users to own and establish the provenance of the digital data they create. Users, however, still need to be authenticated, necessitating a detailed examination of the authentication model employed in these schemes.

Interesting solutions have been suggested for managing users’ authentication and ensuring the integrity of the digital data they create. Such systems can be categorized into three classes based on their characteristics: they either retain all information on the ledger, keep only the hash, or involve a third party that can be fully or partially trusted. Each option has its benefits and drawbacks, which influence the choice of a specific approach in the proposed solutions.

8. Conclusion

Blockchain technology revolutionizes the way digital information is shared and protected. Its novel approach to authentication and integrity is remaking systems across industries. The advent of blockchain technology, with its capacity to forge dependable digital identities and offer trusted ledger services, is gradually changing the course of numerous industries, from the financial sector to the energy market. Academic research on blockchain technology has mainly concentrated on topics like consensus algorithms, multi-chain systems, energy-consumption models, and smart contracts. However, authentication and data integrity have been largely overlooked.

This research details frameworks based on blockchain technology that authenticate identity and safeguard data integrity. Existing methods of verifying identities and securing information are analyzed, along with the integration of blockchain into these approaches. Past research has often overlooked how users authenticate themselves with products. Consequently, frameworks are proposed that grant authenticated access to data or digital copying of goods; such approaches add a new security dimension to the conventional problem of data integrity (Zolanvari et al., 2018).

References:

1. Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2019). Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials*, 21(1), 446–471. https://arxiv.org/pdf/1810.08735

2. Yao, W., Deek, F. P., Murimi, R., & Wang, G. (2023). SoK: A Taxonomy for Critical Analysis of Consensus Mechanisms in Consortium Blockchain. *IEEE Access*, 11, 79572–79587. https://arxiv.org/pdf/2102.12058

3. Zhang, X., Xue, M., & Miao, X. (2022). A Consensus Algorithm Based on Risk Assessment Model for Permissioned Blockchain. arXiv preprint arXiv:2207.07453. https://arxiv.org/pdf/2207.07453

4. Gilda, S., Jain, T., & Dhalla, A. (2022). None Shall Pass: A blockchain-based federated identity management system. arXiv preprint arXiv:2207.02207. https://arxiv.org/pdf/2207.02207

5. Jodeiri Akbarfam, A., Barazandeh, S., Maleki, H., & Gupta, D. (2023). DLACB: Deep Learning Based Access Control Using Blockchain. arXiv preprint arXiv:2303.14758. https://arxiv.org/pdf/2303.14758

6. Rouhani, S., Belchior, R., Cruz, R. S., & Deters, R. (2020). Distributed Attribute-Based Access Control System Using a Permissioned Blockchain. arXiv preprint arXiv:2006.04384. https://arxiv.org/pdf/2006.04384

7. Baldi, M., Chiaraluce, F., Kodra, M., & Spalazzi, L. (2019). Security analysis of a blockchain-based protocol for the certification of academic credentials. arXiv preprint arXiv:1910.04622. https://arxiv.org/pdf/1910.04622

8. Jodeiri Akbarfam, A., Heidaripour, M., Maleki, H., Dorai, G., & Agrawal, G. (2023). ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability. arXiv preprint arXiv:2308.03927. https://arxiv.org/pdf/2308.03927

9. Daniel, E., & Tschorsch, F. (2021). Towards Verifiable Mutability for Blockchains. arXiv preprint arXiv:2106.15935. https://arxiv.org/pdf/2106.15935

10. López-Pimentel, J. C., Morales-Rosales, L. A., & Monroy, R. (2021). RootLogChain: Registering Log-Events in a Blockchain for Audit Issues from the Creation of the Root. *Sensors*, 21(21), 7161. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8621924/

11. Ramachandran, A., & Kantarcioglu, M. (2017). Using Blockchain and Smart Contracts for Secure Data Provenance Management. arXiv preprint arXiv:1709.10000. https://arxiv.org/pdf/1709.10000

12. Newell, J., Mamun, Q., ur Rehman, S., & Islam, M. Z. (2021). A Generalised Logical Layered Architecture for Blockchain Technology. arXiv preprint arXiv:2110.09615. https://arxiv.org/pdf/2110.09615

13. Truong, N. B., Sun, K., & Guo, Y. (2019). Blockchain-based Personal Data Management: From Fiction to Solution. In *2019 IEEE International Conference on Blockchain* (Blockchain), 32–39. https://arxiv.org/pdf/1908.10630

14. Liu, C., Guo, H., Xu, M., Wang, S., Yu, D., Yu, J., & Cheng, X. (2021). Extending On-chain Trust to Off-chain: Trustworthy Blockchain Data Collection using Trusted Execution Environment (TEE). arXiv preprint arXiv:2106.15934. https://arxiv.org/pdf/2106.15934

15. Zhang, R., George, A., Kim, J., Johnson, V., & Ramesh, B. (2019). Benefits of Blockchain Initiatives for Value-Based Care: Proposed Framework. *Journal of Medical Internet Research*, 21(9), e13595. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6789420/

16. Umoren, O., Singh, R., Pervez, Z., & Dahal, K. (2022). Securing Fog Computing with a Decentralised User Authentication Approach Based on Blockchain. *Sensors*, 22(9), 3387. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9143246/

17. Kang, I., Gupta, A., & Seneviratne, O. (2022). Blockchain Interoperability Landscape. arXiv preprint arXiv:2212.09227. https://arxiv.org/pdf/2212.09227

Cite this Article

Shubham Sharma *&* ***Er. Abhay Dwivedi*** *"****Blockchain-Based Authentication and Data Integrity Frameworks****", International Journal of Engineering, Technology and Computer Science, ISSN (Online): Applied, Volume 1, Issue 1, pp. 30-40, October - December 2025.*

Journal URL: *https://ijetcs.com/*