Mesopotamian journal of Cybersecurity
Vol.5, No.3, **pp**. 1081–1108
DOI: https://doi.org/10.58496/MJCS/2025/058; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Review Article

Blockchain-Based Accountability: A Systematic Literature Review

Nabeel Z. Tawfeeq[1, *], Dujan B. Taha[1,]

[1] *College of Computer Science and Mathematics, University of Mosul, 41002 Mosul, Iraq*

ARTICLEINFO

Article History

Received 7 Jul 2025
Revised 29 Aug 2025
Accepted 04 Sep 2025
Published 8 Oct 2025

Keywords

Blockchain
Accountability
Traceability
Smart Contract

ABSTRACT

The Blockchain algorithm has advanced the accountability and transparency of modern digital infrastructures. Enforcing responsible behavior and data integrity across distributed environments involves several key components, such as smart contracts, access control models, cryptographic techniques, and a decentralized identity framework. Because the blockchain ledger is immutable and transparent, once a transaction is recorded, it cannot be altered without detection, making fraudulent actions easily traceable and thereby ensuring accountability. However, the need for hybrid approaches that combine on-chain and off-chain solutions for an efficient reliability system introduces challenges, including privacy preservation, scalability, and regulatory compliance. This paper analyzes the effective features that enhance blockchain accountability, such as immutability, traceability, auditability, and decentralized control. We propose research gap directions for the research community. To improve the reliability of blockchain systems across various domains, based on a systematic analysis and integration of recent developments and real-world demands. Consequently, we have distinguished 33 relevant research studies from a total of 358 publications covering the period between 2020 and 2025 by employing the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. We identified three major themes addressed by the papers in the reviewed studies: further investigations into the ML role in enhancing accountability are required, especially using lightweight ML algorithms such as BNN and Tseltin machine, examining the limitations of blockchain's auditability for real-time applications and decision-making efficiency, and a practical study of mechanism scalability in trade-off cost-efficiency.

1. INTRODUCTION

In the contemporary global economic landscape, blockchain technology has emerged as a pivotal mechanism for eliminating the need for trusted intermediaries. The initial demonstration of its practical applicability was put forth by the individual known by the pseudonym Satoshi Nakamoto with the creation of Bitcoin [1]. Shortly thereafter, Ethereum was introduced in 2015, serving as a platform that facilitates the development of smart contracts and decentralized applications. With its smart contracts embodied properties such as transparency and immutability, yielding an auditable record of transactions [2], [3]. Scholars quickly recognized these virtues: Pilkington (2016) and others describe blockchain as a public ledger that inherently boosts visibility and trust [4]. Similarly, note blockchain's capacity to make transactions open and verifiable. By 2018–19, this link to accountability was explicit: governance scholars (e.g., Beck et al. 2018) and case studies (Batubara et al., 2019) emphasize that blockchain is "heralded for improving trust" and can promote transparency and accountability in applications such as public registries [5]. This allows for peer-to-peer transactions without the need for intermediaries [6]. The arrival of Ethereum marked a new era of growth for the cryptocurrency world.

*Corresponding author. Email: nabeel.tawfeeq@uomosul.edu.iq

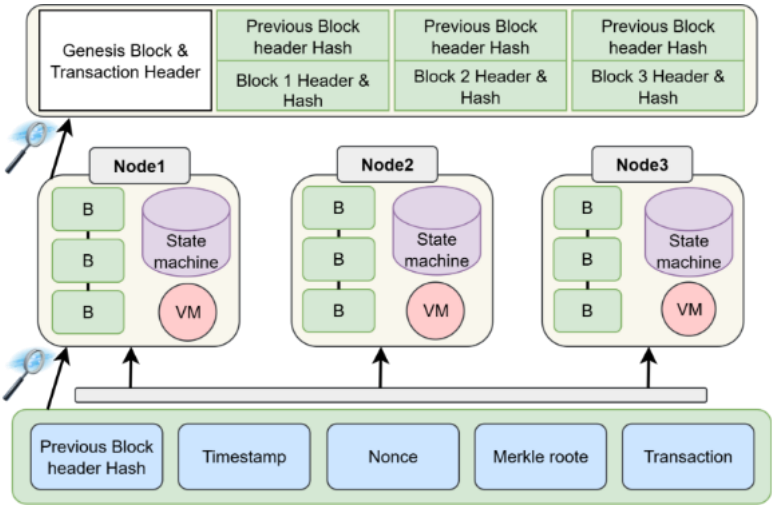

Fig. 1. The blockchain structure and the contents of a block

Unlike Bitcoin, which is primarily used as a medium of exchange, Ethereum offers a powerful platform for developing decentralized applications (dApps) and executing smart contracts, which are self-executing contracts with the terms of the agreement embedded directly into the code. It provides a tremendous number of applications, from decentralized finance (DeFi) sites to Non-Fungible Tokens (NFTs), revolutionizing online agreements and transactions. Functioning as an immutable and decentralized digital ledger, the blockchain ensures that each transaction record is permanently embedded within the system, resistant to alteration or deletion once validated. Although initially developed to support cryptocurrencies, its application has since expanded significantly, demonstrating substantial potential in various sectors due to its robust security, transparency, and privacy-preserving characteristics.

As a fundamental architecture for the safe, open, and responsible management of data, blockchain technology's versatility is especially evident in its convergence with emerging technological sectors, such as the Internet of Things (IoT), electric vehicles (EVs), financial technology (FinTech), and healthcare infrastructures [7]. Blockchain systems employ a range of cryptographic primitives and consensus mechanisms to safeguard the system's integrity and privacy, while also being able to withstand a variety of adversarial threats with diverse objectives and capabilities [8], [9]. This convergence of blockchain with critical technological infrastructures highlights the importance of systematically examining its role in enhancing accountability mechanisms, an area of growing academic and industrial interest [10].

In recent years, blockchain has emerged as a promising technology that automatically records and verifies transactions [11], [12]. In simple terms, blockchain is a cryptographically secure protocol for creating an immutable digital data structure that tracks asset transactions between members of a public or private peer-to-peer network. The key characteristics of the blockchain include transparency, trust, speed, and the elimination of a single point of failure in centralized systems. The distributed framework that blockchain presents facilitates the simultaneous connection of multiple computers, enabling them to access the requisite information efficiently [13]. Additionally, it is used to enhance data security and immutability. Smart contracts and consensus mechanisms are implemented to maintain the integrity and transparency of stored traffic data [14]. Consequently, this paradigm shift transitions data management from a centralized model to a decentralized and transparent approach, which simultaneously enhances data security [11].

Despite operating in a decentralized manner, the distinctive characteristic of blockchain technology lies in the creation and preservation of hash values within the blocks of the blockchain network. Each block includes the hash of the previous block. This chained-hash system ensures that any alteration in one block will affect all subsequent blocks, making unauthorized changes highly detectable, as shown in Fig. 1. Furthermore, it helps to maintain the validity of the entire blockchain, making it a strong means to update records in various fields such as education and finance [15]. Blockchain is well-known for its integrity and ability to facilitate secure solutions; therefore, it is an effective tool for providing traceability. New advances in this technology have had a significant impact on traceability systems. One of the key components of track and trace systems is the ability to trace a product's origin and source. The recorded events are essential for understanding how blockchain can be used to establish traceability, as demonstrated by research across various

industries [16]. These use cases illustrate the potential of blockchain technology to enhance transparency and accountability in supply chains, ultimately leading to increased efficiency and trust.

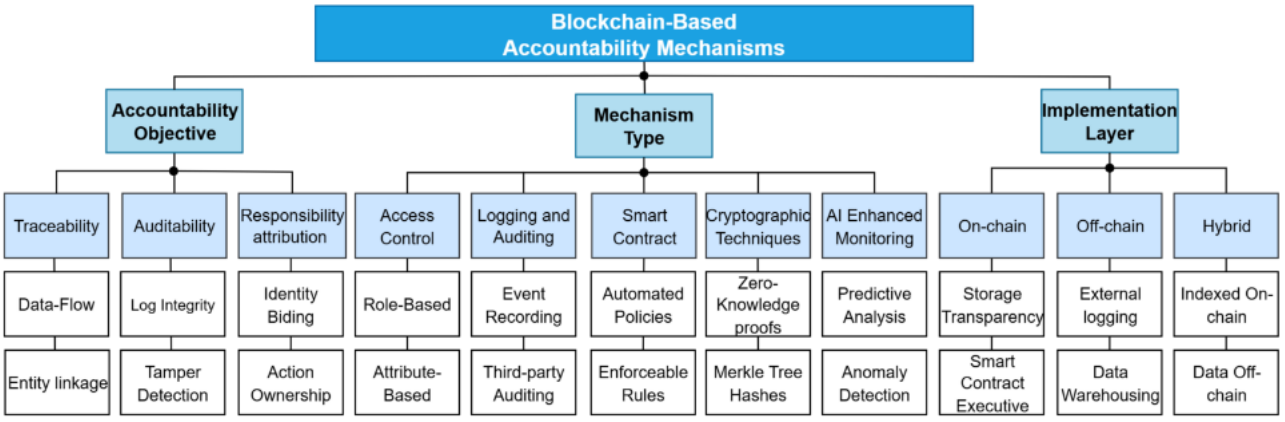

Fig. 2. Taxonomy of blockchain-based accountability mechanisms

Researchers have long sought to create digital systems that are both robust and accountable by integrating machine learning approaches, such as BNNs and TMs, to enhance the accountability of blockchain systems [17], [18], [19]. Additionally, AI-driven detection techniques, such as intrusion detection systems, can significantly strengthen trust and resilience in networked systems [20]. Furthermore, some research emphasizes the need to balance efficiency and security in resource-constrained environments, such as those in the AES [21], [22].

In this paper, our goal is to provide an extensive review of the existing knowledge on blockchain-based accountability mechanisms, with a focus on auditing, traceability, and transparency across various industries. The issues of corruption and improving transparency within governance systems are of paramount importance. Through the synthesis of existing literature, our focus is to delineate best practices and recommend pragmatic guidelines for augmenting accountability in the implementation of blockchain technologies. By responding to pertinent research inquiries utilizing a method that incorporates a sequenced framework for executing a systematic literature review (SLR). [23], we endeavor to contribute to this discourse. Following the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses.* (PRISMA) criteria for SLR, thirty-three foundational publications are examined. The PRISMA statement provides prescriptive recommendations for systematic reviews, encapsulating advancements in the identification, selection, evaluation, and synthesis of studies [24]. This paper contributes the following:

- A comprehensive SLR utilizing the PRISMA methodology. The study analyzes over 358 recent publications from the digital library publications (2020-2025). Additionally, 33 of the relevant articles served as the primary source for data analysis. This approach ensures transparent analysis of relevant research, providing an aggregation and synthesis of recent findings.
- In-depth exploration of the core features, such as immutability, traceability, and auditability, that are centric mechanisms related to blockchain-based accountability. This analysis bridges the gap between technical capabilities and data integrity and transparency in distributed systems.
- A comprehensive synthesis of the domain's prospects, challenges, and future directions, highlighting the key barriers (privacy, scalability, and regulatory compliance issues), proposing solutions, and identifying research gaps to advance blockchain-based accountability across various domains.

Furthermore, this SLR offers a comprehensive and thorough examination of the subject concerning blockchain-based accountability mechanisms, organized around three established themes, as shown in Fig. 2: accountability objective, mechanism type, and implementation layer. The subsequent sections of the article are organized as follows. In Section 2, we elucidate the pertinent literature in the context of the research study. In Section 3, we explicate our methodological framework and procedural approach. Furthermore, in Section 4, we will articulate and execute a critical evaluation of the three main themes that have emerged from this systematic review of the literature. Section 5 explores the empirical validation and real-world cases across the reviewed studies. Section 6 presents a detailed examination of the findings related to the research questions, while Section 7 outlines the challenges encountered and the research gaps identified, along with

a series of recommendations and prospective avenues for future inquiry. Finally, Section 8 offers a conclusive summary of this SLR.

2. RELATED SURVEY

Several systematic reviews and survey studies have examined blockchain technology from diverse perspectives, such as accounting, auditing, governance, education, and supply chain management; however, these contributions remain broad in scope and only tangentially address accountability mechanisms. In Table I, we showcase a summary of the aims of past reviews. Examining the impact of blockchain on accounting, auditing, and security is included in [25]. However, the choice between permissioned and permissionless blockchain affects security and throughput. Moreover, [26] identifies multiple definitions and measurements of centralization. [27] focused on blockchain and governance topics. In addition, [28] reviewed blockchain solutions applied in the educational landscape, focusing on diploma falsification prevention and solutions. Limited frameworks exist for diploma generation, verification, and revocation. Lastly, [29] discusses security challenges and issues in blockchain. Additionally, the characteristics of blockchain, including decentralization, transparency, and immutability, are investigated. A thorough examination of blockchain applications within livestock supply chains underscores their potential to improve transparency, traceability, and accountability. The study addresses issues such as fraud, inefficiencies, and data manipulation that are prevalent in conventional systems by leveraging blockchain's decentralized and immutable framework [30]. However, existing blockchain surveys have not adequately addressed accountability mechanisms. For example, [31] investigates the impact of blockchain on the accounting, auditing, and accountability domains. However, their analysis remains general, emphasizing efficiency and transparency rather than detailing how accountability is enforced. Many other surveys focus on specific application areas (such as education diplomas, supply-chain tracking, and sustainable finance). They may mention improved transparency or traceability, but they treat accountability only peripherally. The following points briefly summarize the limitations of prior blockchain reviews.

- Broad-thematic reviews: Prior SLRs on blockchain (accounting, auditing, governance) cover general benefits like transparency and trust, but do not systematically analyze accountability tools [32].
- Domain specific reviews: Many reviews focus on specific sectors (education credentials, agri-food supply chains, etc.). These discussions address problems such as fraud or counterfeit prevention, but none undertake a cross-domain analysis of blockchain accountability mechanisms.

Together, these points show that earlier surveys have not addressed blockchain accountability mechanisms in depth. They either treat accountability as a side issue or omit it entirely. In contrast, our new SLR is dedicated specifically to blockchain accountability.

TABLE I. A SUMMARY OF THE PAST RELATED SURVEY

Ref.	Focus	Dataset
[25]	Blockchain's impact on accounting, auditing, and AI integration.	Analyzed a dataset of 179 articles on BC and accounting.
[26]	Highlights increased centralization trends in cryptocurrencies like Bitcoin.	Research papers published between 2009 and 2019.
[27]	Accountability mechanisms in governance are identified and categorized.	Analyzed 510 publications from various databases.
[28]	Reviews blockchain technology for diploma verification in education.	1744 papers published between 2018 and 2022.
[29]	Surveys blockchain technology's evolution and architecture.	Review blockchain characteristics and challenges.
[30]	Analyzes the present condition of blockchain applications in livestock.	Not mentioned in the survey.

3. RESEARCH DESIGN

3.1 Procedure

We adhered to the protocols delineated by [24] to execute this SLR. The primary objective is to identify the most effective methodologies through data analysis. This approach necessitates the formulation of focused and precise inquiries while conforming to a stringent set of guidelines. Our investigative methods employed a comprehensive four-step PRISMA framework to guarantee that all pertinent studies were discerned and assessed. Fig. 3 illustrates the complete search procedure.

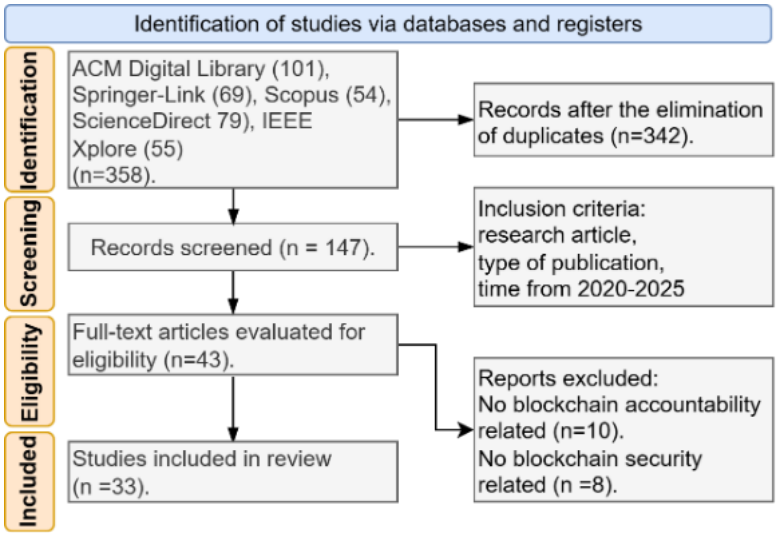

Fig. 3. PRISMA search methodology

Our methodological framework employed a systematic four-step PRISMA protocol to ascertain that all relevant studies were comprehensively identified and appraised. The initial phase of the PRISMA methodology involved formulating a research protocol, which encompassed establishing a research question, delineating a comprehensive set of search terms, and identifying pertinent bibliographic databases for the search. The second phase entailed the application of the inclusion criteria, while the third phase involved the implementation of the exclusion criteria. The entire process culminated in the collection and rigorous analysis of the data. The research questions (RQs) that will guide this study are delineated as follows:

RQ1: What are the existing approaches to implementing auditability and traceability in blockchain-based accountability frameworks?
RQ2: How do smart contracts contribute to enforcing accountability in decentralized systems?
RQ3: What role does access control play in strengthening trust and responsibility in blockchain-enabled infrastructures?
RQ4: What are the strengths and limitations of current models combining these mechanisms for accountability enhancement?

3.2 Search Strategy and Data Collection

For our investigation, we employed the following online research databases and search engines: ACM Digital Library, IEEE Xplore, SpringerLink, Scopus, and ScienceDirect. The terms utilized in our queries are enumerated in Table II. In formulating a search query, each cluster of keywords is interconnected through the OR operator, whereas the clusters themselves are amalgamated using the AND operator. The second stage of our search strategy is the screening phase, during which we apply the inclusion criteria. At this stage, the studies deemed pertinent were selected by the subsequent criteria, following a systematic and rigorous process:

- The manuscript in question must constitute a scholarly paper that has either been presented at an academic conference or disseminated in a journal subject to the rigors of peer review;
- The manuscripts must have attained publication status at any point within the temporal parameters of 2020 to 2025
- The manuscripts must be composed in the English language.

This determination is based on the insights and contextual framework derived from previous investigations. The methodologies employed in scholarly articles disseminated prior to 2020 were insufficiently suited to address specific research inquiries.

3.3 Relevant Studies Selection

At stage 3 of the application of the exclusion criteria, studies that were not about blockchain (accountability, transparency, traceability, or enhancing blockchain-based accountability mechanisms) were eliminated.

TABLE II. RELATED SEARCH QUERY

“Blockchain” OR “Distributed Ledger”
AND
“Accountability” OR “Auditability”
AND
“Enhancing” OR “Framework”
ND
“Access Control” OR “Smart Contract”

At this juncture, a comprehensive analysis was conducted on all titles, abstracts, and keywords to determine the suitability of the papers for the subsequent phase. Moreover, following a thorough examination and assessment of the pertinent articles, it was disclosed that thirty out of the forty-three articles were either lacking complete texts or consisted of narrative review papers, which did not provide meaningful insights into the mechanisms of blockchain-based accountability. As a result, those papers were disqualified, which brought the total number of relevant papers to 33. In Table III, we present the aggregate quantity of the selected studies identified in the final phase. The table indicates that the preponderance of scholarly articles originates from IEEE Xplore, comprising 21 articles, followed by Scopus with a total of 5 articles, then ACM DL and ScienceDirect with 3 articles each, and finally, SpringerLink with 1 article. Out of the 33 scholarly articles, 19 were journal papers, while 14 were conference articles. An exhaustive overview of the pertinent literature, including their descriptions and their relation to the research inquiries, is presented in Table IV.

3.4 Restrictions and Threats to Validity

Any scholarly inquiry involves numerous constraints. Several elements require consideration when evaluating this SLR, as they may significantly impact the validity of the results. These elements encompass:

- Only articles composed in the English language were selected for inclusion in the study. During our examination of the research databases, we identified pertinent articles in alternative languages; however, these articles were ultimately excluded from the analysis due to their language.
- The articles included in the study were sourced solely from the five digital research databases shown in Fig.3. Therefore, it is plausible that we missed publications that were cataloged in different digital repositories. • The study exclusively included peer-reviewed journal articles and conference proceedings. Non-peer-reviewed scientific investigations were excluded from the analysis. This exclusion encompassed brief articles, experiential reports, and assimilation studies, which generally present ongoing work or preliminary investigations deemed minimally relevant to the field. Publications released before 2020 were excluded because there was an insufficient number of relevant studies available to address the research questions, critically evaluate the evidence, and support valid conclusions. Only works published between January 1, 2020, and November 27, 2025, were included. Some conference papers

presented before December 27, 2025, may not have been published by the study cut-off date and were therefore omitted from the literature review.

4. THEME-BASED SYNTHESIS

The thematic analysis represents a highly adaptable methodology for qualitative research, allowing the discernment and interpretation of recurring themes within the datasets. The SLR methodology requires a comprehensive articulation to ensure that literature reviews possess integrity and can be independently replicated. This diligence ensures that the resultant findings are credible and subject to validation by other scholars, thereby enhancing the overall caliber of the scholarly endeavor [66]. The methodological rigor inherent in thematic analysis plays a crucial role in bolstering the trustworthiness and replicability of qualitative research outcomes, thereby aligning with the overarching criteria of research excellence. The methodical implementation of thematic analysis not only enhances the credibility of qualitative investigations but also facilitates a deeper understanding of complex data patterns.

TABLE III. THE DISTRIBUTION OF ARTICLES WITHIN REPOSITORIES.

IEEE Xplore	ACM DL	ScienceDirect	Springer-Link	Scopus
21 Paper	3 Paper	3 Paper	1	5

TABLE IV. A SUMMARY OF THE STUDIES AND THEIR CORRELATION WITH THE RQS.

Studies	Objective	Relations to RQs
[33, 34]	Implement access control in blockchain systems.	RQ3
[35–38]	Improve auditability and traceability.	RQ1
[39–41]	Token frameworks, reputation mechanisms.	RQ1, RQ3
[42]	Enhance security in file integrity monitoring systems.	RQ1
[43]	Develop a secure system for tracking products.	RQ1, RQ2
[44]	Used cryptographic primitives to enhance diploma.	RQ1
[45]	Provide verifiability and anonymity for buyers.	RQ1, RQ3
[46]	Introduce audit layer to protect log integrity.	RQ1, RQ2
[47]	Improve data transparency in ESG reporting.	RQ4
[48]	Design auditable federated learning framework.	RQ1
[49]	Audit systems to analyze models limitation.	RQ1, RQ2, RQ4
[50–52]	Develop smart contract-based systems verification.	RQ1, RQ2, RQ3, RQ4
[53]	Design an audit data traceability and verification.	RQ1
[54]	Present blockchain-based multi-cloud data auditing.	RQ1
[55]	Prove data verifiability and authenticity.	RQ1, RQ2
[56]	Develop a decentralized tool for transparency.	RQ1, RQ2
[57]	Basic data model for a generic traceability system.	RQ1, RQ2
[58]	Secure blockchain-based audit log system.	RQ1, RQ2
[59]	Hyperledger Fabric for enhancing security in HDFS.	RQ1
[60]	Combined (MA-ABE) with blockchain technology.	RQ2
[61]	A Verification model for data marketplaces.	RQ1
[62]	Accountable fine-grained blockchain framework.	RQ3

[63]	Explore real-life scenarios for smart contracts.	RQ2
[64]	Used cross-border data sharing and anonymity.	RQ1, RQ2
[65]	Smart contracts to improved system performance.	RQ2

4.1 Theme 1: Accountability Objective

In blockchain technology, accountability can be achieved via multiple aspects (traceability, auditability, and responsibility attribution) [47]. These dimensions provide a robust analytical framework for categorizing and interpreting current research on improving blockchain-based accountability mechanisms [60]. Traceability in the blockchain context refers to the ability to track assets, transactions, and actions in a transparent and immutable manner, ensuring that all data is verifiable and tamper-proof [58]. Traceability is essential for fostering transparency and accountability across various sectors [49]. Block headers maintain integrity and traceability within a blockchain [67]. As Fig. 4 shows, each block header stores the following elements:

- Pre-block hash value: Reference to the previous block's hash, ensuring continuity and preventing unauthorized alterations.
- Current block hash: A unique identifier for the current block, derived from the stored data.
- Timestamp: A record of when the block was created, aiding in tracking information flow over time.
- Merkle root: The Merkle root represents a cryptographic hash encompassing all constituent nodes of a Merkle tree [48]. As illustrated in Fig. 4, within the context of a blockchain block, it serves as the aggregated hash of the transactions contained within that block. Merkle trees are extensively employed to authenticate large data structures in a manner that is both secure and efficient. The Merkle root within a blockchain is located in the block header segment of a block, functioning as the hash that encapsulates all transactions within that block. Consequently, it suffices to verify the Merkle root solely in order to confirm the validity of all transactions represented in the Merkle tree, thereby obviating the need to verify each transaction individually.

Several studies employ the intrinsic characteristics of blockchains, namely immutability, transparency, and decentralization, to implement traceability mechanisms in various domains. Immutable logs are commonly used to record data usage activities in tamper-proof ledgers, supporting transparent auditing and policy compliance [36].

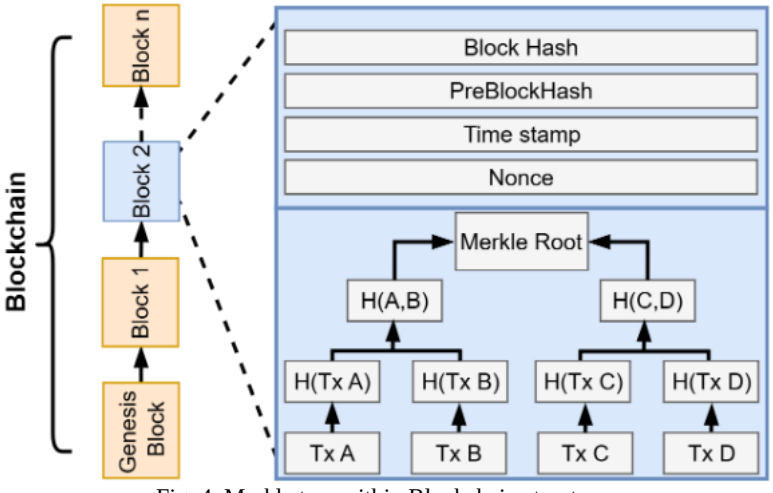

Fig. 4. Merkle tree within Blockchain structure.

This property is central to maintaining the integrity of the message because it protects the data from tampering. The blockchain achieves this by cryptographically linking blocks, so any change in previously added data will break the chain and be easily detectable [67]. On the other hand, tokenization techniques enable the tracking of user activity by embedding identity-specific information within tokens, particularly in redactable blockchain environments [53]. Data lineage

approaches utilize cryptographic methods to ensure reliable data update and storage tracking, thus improving audit trail consistency [49]. Furthermore, smart contracts and NFTs facilitate secure and intermediary-free transaction histories that reinforce data provenance, notably in IoT and charitable applications [51].

Some studies propose blockchain-based frameworks that enforce data usage policies through smart contracts, maintaining verifiable records of data interactions. Furthermore, audit data systems integrate blockchain with deep learning to improve the traceability and verification of collected audit data. Taken together, these methods underscore the versatility of blockchain in supporting traceability across various sectors, including healthcare, supply chain management, and data management. Every block in the chain contains a unique cryptographic hash, a string generated from the data in that block. This hash is like a digital fingerprint for the message. If even a small change is made to the message, the fingerprint changes drastically, indicating that tampering has occurred. These hashes are also linked from one block to the next [68]. Before a new message or transaction is added to the blockchain, network nodes work together to verify that the message is legitimate. This agreement process is known as consensus [69]. With multiple parties checking each message, it becomes extremely difficult for a single malicious actor to introduce altered or fake data into the chain [70]. However, challenges such as data scalability and privacy leakage through metadata remain recurring concerns that require further research and optimization.

The second aspect of the accountability objective is auditability. Conventional centralized audit log systems encounter considerable difficulties in maintaining data integrity due to vulnerabilities such as log injection attacks and single points of failure. These systems often rely on a single logger or auditor, which is susceptible to compromise, potentially leading to privacy breaches or collusion [46]. Fig. 5 Illustration of audit logging: In (a), a legitimate logger records actions, while in (b), a compromised logger fabricates or omits logs. Blockchain's distributed nature allows audit logs to be processed and replicated across a network of peers, enhancing consistency and security. This approach provides a defense against log injection attacks and reduces the risk of single-point failures [46]. Auditability constitutes a significant attribute [71] since no individual should possess the capacity to engage in misconduct, such as the assignment or revocation of a role, without the awareness of the other involved parties, nor should any entity be able to disavow the actions they have undertaken [72].

Some blockchain systems assume a general threat model in which nodes, including loggers and auditors, are considered untrusted. As shown in Fig. 6, these systems utilize multiple nodes for logging and auditing, employing consensus algorithms to mitigate compromise and collusion attacks, ensuring a more secure and reliable log system [36]. Techniques such as chameleon hashing are used in auditing methods to detect tampering. This method enables quick determination of data integrity without examining specific content, making it efficient for detecting unauthorized changes [36].

In some systems, Hyperledger Fabric is used to prevent log tampering [69]. The logger processes log files using chain code executed in secure Docker containers, with multiple endorsers following an endorsement policy to ensure consensus before updating the blockchain [46].

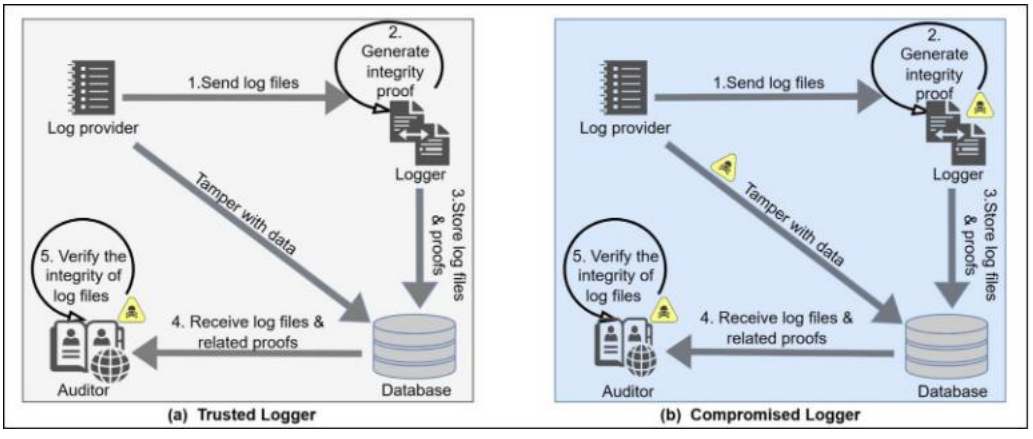

Fig. 5. (a) Conventional audit system. (b) Threat audit system.

Various mechanisms have been proposed and implemented in the reviewed literature to ensure responsibility attribution in blockchain-based environments. Smart contracts and digital signatures in non-fungible token (NFT) transactions enable strong identity binding and action ownership, providing cryptographic verification of ownership and reducing disputes over duplication or unauthorized transfers [49], [10]. In blockchain-based auctions, anonymity is preserved through

cryptographic protocols while maintaining accountability for actions. Bids are securely attributed to anonymous yet verifiable identities, promoting fairness and deterring manipulation [49].
Similarly, accountability in blockchain governance is reinforced through transparent and immutable ledgers that bind actions to pseudonymous identities, enabling traceability and promoting responsible behavior among participants [73]. Case studies such as Ethereum and the Lido protocol demonstrate how on-chain accountability mechanisms formalize action attribution to stakeholders, navigating the balance between transparency and operational security [74]. Furthermore, multi-signature schemes—particularly in charitable NFT auctions—demand authorization from multiple parties for transaction execution, thereby ensuring collective action ownership and mitigating fraudulent behavior through consensus-based validation [10].

4.2 Theme 2: Mechanism Type

A review of the selected literature reveals that the Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) mechanisms are widely adopted to enhance security and privacy across multiple domains, notably in healthcare and financial technology. These access control models are used to enforce fine-grained authorization policies, thereby ensuring that data access is limited to authorized entities based on defined roles or attributes. The Medical Records Data Accountability and Compliance (MRDACE) architecture implements RBAC by assigning predefined roles, such as patients, doctors, and researchers, with specific permissions managed through smart contracts. This ensures that only authenticated and authorized users can access sensitive medical data [75].
Another research uses RBAC to ensure that specific data and actions are accessible only to authorized users, streamlining user permissions management and improving security and efficiency [10]. Numerous scholarly investigations demonstrate the implementation of ABAC frameworks to improve data privacy and secure access within blockchain-oriented systems [50]. Li et al. proposed a patient-centered access control architecture that utilizes multi-authority Attribute-Based Encryption (ABE) for managing access to Personal Health Records (PHRs) hosted on semi-trusted servers. Each individual patient's PHR is encrypted autonomously to preserve confidentiality and implement fine-grained access control [75]. In a similar vein, Wu et al. presented a privacy-preserving and traceable blockchain paradigm wherein attribute-based encryption protects user data and facilitates identity traceability, thus achieving a balance between privacy and accountability [36].
The processes of logging and auditing serve as fundamental frameworks within the context of accountability facilitated by blockchain technology, guaranteeing that system interactions are documented in a manner that is both immutable and transparent. These processes are essential for establishing verifiable records concerning the use of data, identifying irregularities, and reinforcing adherence to operational and legal standards. To establish robust accountability within such environments, it is essential to implement several interconnected mechanisms, including:

- **Event Recording:** Multiple studies emphasize the importance of log files as a primary source of forensic evidence for assessing system reliability and detecting misconduct. Traditional logging methods, however, are susceptible to tampering. To address this, blockchain has been integrated to ensure tamper-proof, distributed, and verifiable event logs. These immutable logs are particularly valuable in cloud environments, where they are used to resolve disputes and verify compliance with Service Level Agreements (SLAs) [76]. Smart contracts further automate this process by validating contractual terms and triggering actions based on logged events [46].
- **Third-Party Auditing:** The traditional reliance on reputable third-party auditors (TPAs) for verifying integrity has come under scrutiny due to issues surrounding trust and transparency. To alleviate this reliance, blockchain-oriented auditing frameworks have been developed. These innovative systems employ smart contracts to autonomously authenticate data integrity and audit trails, thereby obviating the necessity for external TPAs. The transparency and immutability provided by blockchain technology guarantee that all auditing activities are both traceable and verifiable in real-time [53]. These blockchain-enabled logging and auditing solutions enhance accountability by providing consistent, verifiable, and decentralized records of system activities. Despite their benefits, challenges such as scalability, performance overhead, and real-time responsiveness remain areas for further research [77].
- **Blockchain-Enabled Data Accountability:** Smart contracts facilitate the codification of Event-Condition-Action (ECA) protocols, which autonomously implement data utilization regulations. As Fig. 7 illustrates, one common approach for encouraging data accountability and provenance tracking is rooted in policy-based contracts between data subjects and service providers. These models generally separate implicit and explicit data, which can be gathered automatically from devices or applications or directly by users. These preemptive measures ensure that confidential information is accessed exclusively under specified, authorized circumstances, thereby reducing the potential for abuse and enhancing system accountability [72].

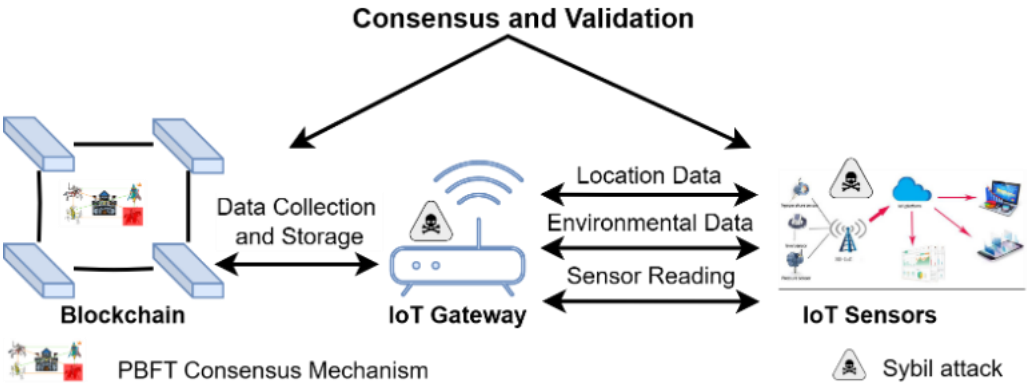

Fig. 6. The integral role of IoT and blockchain technologies, along with the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, in ensuring security and privacy.

- **Automated Governance Enforcement:** Within governance structures, smart contracts facilitate the automatic execution of consensus-based decisions. By eliminating human intervention in critical decision-making processes, blockchain enhances the consistency, impartiality, and transparency of rule enforcement [73].
- **Regulatory Compliance Integration:** In order to fulfill regulatory mandates, numerous blockchain frameworks embed legal and policy stipulations directly within the logic of smart contracts. This integration at the design phase facilitates the maintenance of compliance with external regulatory standards and internal organizational policies, thereby minimizing the potential for fraudulent or non-compliant activities [76].
- **Formal Verification of Smart Contracts:** To augment the reliability and security of smart contracts, formal methodologies, including model-based verification and machine learning-supported analysis, are utilized to authenticate the logical framework of smart contracts. As shown in Fig. 8, these methodologies ensure that contracts are free from vulnerabilities and function as intended, thereby facilitating the reliable automated enforcement of regulations [78].
- **Accountability in Cloud Services:** In the context of the cloud, smart contracts enforce accountability by managing service infractions and performing compensatory functions (e.g., transferring credits) [33]. This self-enforcing capability enhances trustworthiness while reducing operational frustration [79]. Automated policy enforcement through blockchain and smart contracts serves as a robust accountability mechanism across various domains. These technologies ensure that predefined rules are executed consistently and securely, although challenges related to formal verification, legal adaptability, and smart contract upgradability remain areas for future exploration [65].
- **Privacy-Preserving Verification and Data Integrity:** Privacy and data integrity are foundational to accountable blockchain systems, especially in scenarios involving sensitive or cross-border data sharing. Two key cryptographic primitives [61], zero-knowledge proofs (ZKPs) alongside Merkle tree hashing, are extensively employed in the examined scholarly works to realize these aims while ensuring transparency and verifiability [10], [80]. ZKPs facilitate the demonstration of the veracity of information without necessitating the revelation of the associated data. ZKPs enable exactly this: a prover can convince others that a statement is true (e.g., “I have a valid transaction” or “I know a secret key”) without revealing the underlying data within blockchain architectures. ZKPs are utilized for transactions that prioritize privacy, authentication mechanisms, and secure computational processes, thereby ensuring that data utilization remains verifiable while safeguarding user confidentiality. These proofs are frequently combined with sophisticated cryptographic techniques, such as multi-party computation (MPC) and homomorphic encryption (HE), thereby enabling intricate analyses and audits that uphold privacy [64]. For instance, in frameworks for transnational data sharing, ZKPs provide a means for regulatory compliance by offering evidence of authorization while concurrently maintaining the anonymity of users. Although ZKPs can be computationally intensive, recent implementations have tailored-proof systems for specific blockchain applications. These optimized solutions prevent fraudulent behavior by utilizing problems such as the discrete logarithm problem to generate lightweight and verifiable cryptographic evidence [77]. Furthermore, preserving data integrity constitutes a significant challenge; occasionally, Merkle trees are used to determine the integrity of extensive datasets with optimal efficiency. Specific clients authenticate that transactions have been incorporated into a block by validating a Merkle root and associated intermediate hashes, all without necessitating access to the complete dataset [45].

- **AI-Enhanced Monitoring and Accountability:** Predictive Analysis AI-enhanced monitoring significantly impacts accountability by leveraging predictive analysis to anticipate potential issues before they occur. This proactive approach allows organizations to address anomalies and irregularities in real time [81], thereby enhancing the accountability of systems and processes. By predicting potential failures or breaches, AI systems can alert stakeholders, ensuring that corrective actions are taken promptly to maintain system integrity and trust [73]. AI algorithms are capable of identifying deviations from expected behavior, such as fraudulent activities or operational malfunctions, by analyzing patterns in transactional and system-level data. This proactive detection of anomalies enhances transparency, ensuring that actions and transactions comply with predefined rules and protocols. As a result, AI contributes to holding entities accountable by flagging irregularities for further investigation, thus reinforcing trust and integrity within blockchain-based systems.

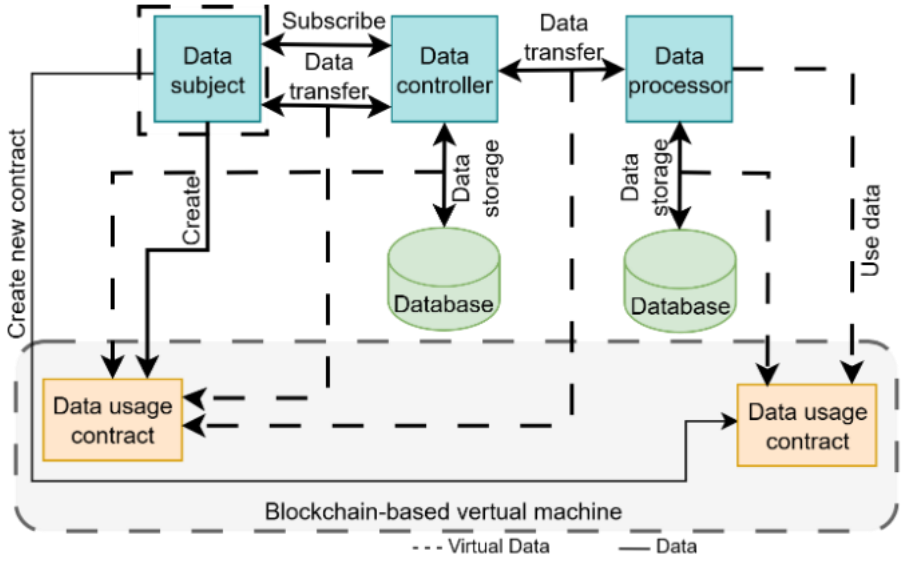

Fig. 7. Blockchain-enabled data accountability structure

4.3 Theme 3: Implementation Layer

The implementation layer in on-chain systems enhances accountability by automating governance decisions through smart contracts. This automation minimizes the potential for human error or manipulation since decisions are executed consistently and impartially once consensus-based rules are established and protocolized [73]. However, this approach also introduces trade-offs, as enhancing accountability for one stakeholder group may inadvertently diminish it for another. The following points summarize these layers:

4.3.1. Off-Chain Accountability

Incorporation with Existing Systems: Off-chain ones, such as those based on cloud infrastructures, utilize blockchain to implement logging and SLA verification, enhancing responsibility without being entirely dependent on on-chain operations [76]. For example, the use of blockchain in political situations, such as the Sierra Leone elections, demonstrates how off-chain applications can increase transparency and accountability in the government [82]. While on-chain solutions provide robust accountability as immutable records, off-chain solutions provide greater flexibility and interoperability with legacy systems, potentially suggesting a complementary relationship between the two approaches. In a hybrid blockchain system, which combines indexed on-chain data with off-chain storage, the implementation layer plays a crucial role in improving accountability. This technique ensures secure and cost-effective data management while adhering to regulatory requirements, such as the General Data Protection Regulation (GDPR). The following points outline the key components of the hybrid solution:

- Data Governance: Hybrid DLTs utilize private ledgers for personal data, with public ledgers offering tamper-proof history, as in the case of the Traent Hybrid Blockchain [83].

- Real-Time Collaboration: Data among public service agencies can be easily shared, improving operational efficiency and combating fraud with a hybrid blockchain setup [84].
- Auditable Systems: Hybrid models can employ consent management systems that detect violations and ensure data protection regulation compliance, thus ensuring accountability in data processing [85].

Although hybrid blockchain models offer significant advantages in terms of accountability and efficiency, ensuring interoperability while managing the complexity of integrating on-chain and off-chain data remains challenging.

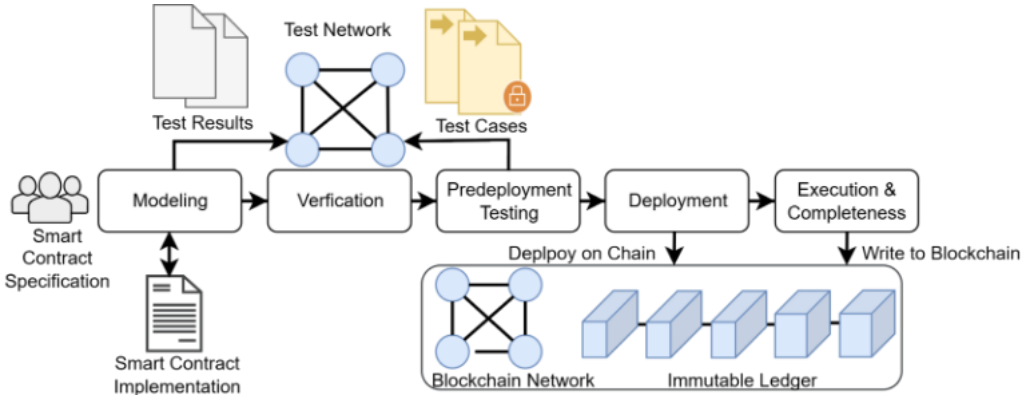

Fig. 8. Extended lifecycle of smart contract development.

4.3.2. Separation of Data and Verification

Off-chain techniques involve storing only essential information, such as metadata or pointers, on the blockchain while maintaining large volumes of raw data in external repositories. This separation ensures that the blockchain records concise references, making it easier to verify that the data was stored and later used appropriately [51]. Fig. 9 presents a proposed solution that leverages blockchain-based mechanisms to enable secure and auditable sharing of private data within smart grid systems. Firstly, by utilizing smart contracts and blockchain technology, a trustless framework has been established for preserving privacy in data computation, allowing fine-grained data usage and access control, tracking non-repudiable data usage, and providing verifiable evidence of policy adherence. After that, an off-chain smart contract execution mechanism has been designed, backed by a Trusted Execution Environment (TEE), and guarantees atomic operations to provide confidentiality in processing user data without inheriting the computational burden of blockchain technology. Through the documentation of metadata, which encompasses unique identifiers and hash pointers, the system is capable of ascertaining the integrity of off-chain data against unauthorized alterations. These hash pointers function analogously to digital fingerprints or receipts, thereby rendering off-chain data accountable to the on-chain ledger. Overall, off-chain methodologies augment the accountability of blockchain systems by ensuring that all essential operations are indirectly documented on-chain through verifiable evidence and metadata, thereby facilitating the establishment of comprehensive audit trails and promoting transparent execution processes of smart contracts.

4.3.3. Immutable Audit Trails

Although unprocessed data remains external to the blockchain, essential transactional information and verification logs are stored within the blockchain itself. This establishment maintains an unalterable audit trail, in which every instance of access, computation, or modification is documented and subject to independent examination. These immutable records are resistant to alteration, thereby guaranteeing that all stakeholders are held accountable for their respective actions. Immutable audit trails secure and make data handling systems more dependable by enabling all modifications to be traced and authenticated in the future. This capability is necessary for regulatory compliance and also generates stakeholder and user trust. The use of blockchain not only provides audit trail integrity but also eliminates the risks of data tampering, thereby improving data governance as a whole. Moreover, the immutable character of blockchain ensures that once records are verified and stored, they cannot be altered, thereby providing a reliable audit trail for companies. This functionality is essential in upholding data integrity and building confidence among stakeholders across various sectors [25].

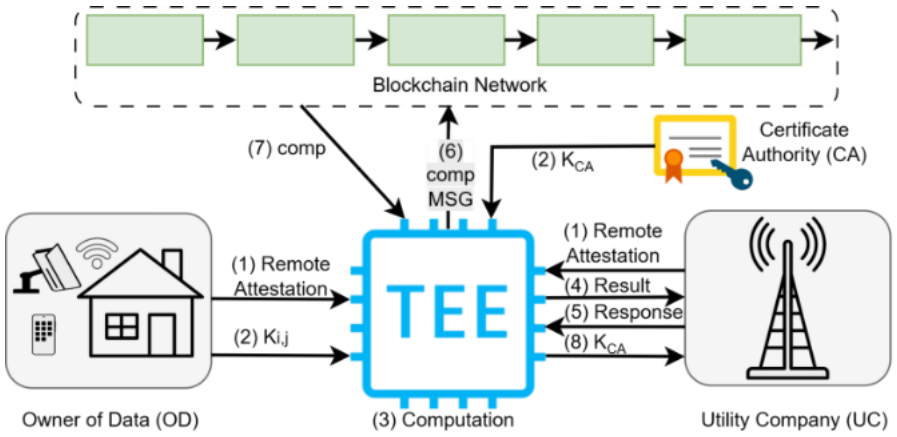

Fig. 9. Off-chain smart contract execution with TEE

5. EMPIRICAL VALIDATION AND REAL-WORLD CASES

Table V shows, the reviewed studies employ diverse validation methods, with a primary emphasis on simulation-based experiments to evaluate performance, scalability, and cryptographic integrity. Accountability mechanisms are empirically validated using simulations, prototypes, or real-world demonstrations. For instance, [51] introduces SPDS, a blockchain-based private data-sharing framework for smart grids, which is validated through extensive simulations that demonstrate improved participant payoffs compared to traditional methods. Similarly, [86] presents a privacy-preserving e-voting framework utilizing zero-knowledge proofs and Merkle trees, evaluated in realistic voting scenarios, which confirms its performance viability. Other studies focus on accountability in data processing. [48] develops a blockchain-based federated learning framework demonstrating effective participant selection through implemented simulations. [54] features a multi-cloud data auditing scheme that detects malicious providers, showcasing practical accountability in cloud storage. Hu et al. introduce Redact4Trace, which maintains on-chain auditing and achieves high accuracy in detecting tampered data [36]. Banu et al. present an SVM-based blockchain framework for financial auditing that significantly outperforms baseline methods in simulated experiments [42].

Collectively, these studies illustrate the breadth of blockchain accountability applications, such as smart grids and electronic voting, with mechanisms validated through empirical evaluation [86]. Furthermore, the integration of cryptographic techniques, including zero-knowledge proofs in Zcash and zk-Rollups on Ethereum, improves privacy and scalability while maintaining accountability [87], [88].

TABLE V. Empirical Validation and Real-World Cases

Study	Validation Approach	Application Domain	Key Outcomes	Limitation
[86]	Use-case demo with 50 voters (ZKP-based e-voting system).	Electronic voting.	Privacy-preserving framework (tamper-evident blockchain ledger, ZKPs for ballot secrecy, Merkle tree storage), Proof generation 8–10s; on-chain verification 500kgas.	Demo limited to 50 voters, Large proving keys (200MB), and High on-chain gas (500k).
[55]	Validation through extensive experimental evaluations, the authors designed two scenarios using real datasets to validate AUDITEM's.	Data integrity verification, particularly within business environments.	Demonstrated the effectiveness in ensuring data integrity verification.	AUDITEM faces scalability and recoverability concerns, particularly with large amounts of data batches.

[57]	Leverages smart contracts on Ethereum Virtual Machine (EVM) for initial testing and validation.	Enhancing traceability within complex supply chains.	Enhances existing classical traceability systems by improving data integrity and automating verification processes.	Lacking broader blockchain network evaluations and Operational costs.
[46]	Hyperledger Fabric prototype (consortium blockchain).	Blockchain-based audit-log integrity (for digital forensics).	50 Percent reduction in on-chain log storage; ensures log integrity under untrusted nodes.	The scalability of blockchain is limited.
[38]	Smart-contract implementation on Ethereum testnet.	Privacy-preserving blockchain transactions (auditable smartcontract transfers).	Privacy-preserving transfer In 4.4s (0.9s proof); formal security proofs of confidentiality and auditability.	Limited in scale and scope.
[48]	Experimental evaluation on a simulated Ethereum network (Remix) with federated model training (MNIST/FashionMNIST).	Federated learning in IoT (distributed ML).	Improves FL model accuracy and convergence speed (vs. random selection).	Selection uses only training-loss (ignores device/computation diversity and efficiency).
[54]	Theoretical security proofs and a prototype implementation.	Multi-cloud storage auditing (cloud computing).	Ensures data integrity and dispute resolution across multiple clouds.	Incurs on-chain storage/gas costs); on-chain overhead remains.
[42]	Simulation-based evaluation: implemented an SVM+Blockchain model in Python.	Financial auditing (finance sector).	SVM-Blockchain (SVM-BC) model significantly outperformed the baselines.	High computational/resource demands.
[62]	Proof-of-concept implementation: built a Python/Charm-based prototype on a simulated 10-node proofof-work blockchain.	Permissionless blockchains.	The prototype showed negligible overhead on chain validation (it acts as an add-on layer without extra consensus cost).	Scalability limits: computation grows with policy size and committee size. For 100 attributes, key generation took 2.4s.

TABLE VI. THE IMPACT OF CONSENSUS ALGORITHM ON ACCOUNTABILITY IN BLOCKCHAIN SYSTEM

Aspect	Impact of Consensus
Signature-based evidence	Algorithms such as Byzantine Distributed Ledger Sharding (BDLS), Practical Byzantine Fault Tolerance (PBFT), and HotStuff utilize cryptographic signatures to authenticate votes and proposals.
Logging and traceability	Certain protocols incorporate verifiable message logs, which may be subjected to audit processes to ascertain the identity of individuals responsible for specific actions and the corresponding timestamps.
Misbehavior detection	In Byzantine Fault Tolerant (BFT) protocols, the mechanisms for achieving consensus are meticulously crafted to withstand and identify nodes exhibiting faults. Reliable nodes meticulously document instances of misconduct to ensure accountability.
Anonymity vs. Responsibility	Proof-of-Work (like Bitcoin) provides pseudonymity but low accountability—you can't easily prove who acted maliciously. BFT systems (like BDLS or Tendermint) offer higher accountability because validators are known.
Punishment mechanisms	In Proof-of-Stake systems, consensus affects how slashing or penalties are applied when a node misbehaves. Strong consensus = enforceable penalties.

6. ANSWERS TO RESEARCH QUESTIONS

The subsequent sections provide a detailed analysis of the findings related to the research questions that were central to this systematic review.

6.1 RQ1: What Are the Existing Approaches to Implementing Auditability and Traceability in Blockchain-Based Accountability Frameworks?

Auditability refers to a system's capacity to produce a complete, accurate, and tamper-resistant record of all operations and transactions. In practice, an auditable system logs every user action and system event, allowing external reviewers to verify its correctness. Blockchains inherently support auditability through their immutable ledgers: each transaction and smart-contract event is permanently recorded, creating an independent, tamper-evident audit trail [89]. Traceability refers to the ability to track the history or origin of an asset or data item throughout a system. Together, auditability and traceability in blockchain systems stem from cryptographic provenance and complete ledger transparency, ensuring that any past transaction can be independently verified and traced. Many existing methodologies leverage smart contracts and immutable logs to augment auditability and traceability within blockchain infrastructures [35]. These techniques support the validation of adherence to SLAs and elevate accountability in cloud operations [76]. These approaches not only streamline auditing processes but also ensure that any violations of SLAs can be effectively identified and addressed. Smart contracts play a pivotal role in implementing auditability and traceability by encoding the logic for data verification and tracking. Various approaches can be utilized to achieve auditability and traceability in blockchain:

- **On-Chain and Off-Chain Data Storage:** One effective approach to balancing scalability and privacy within blockchain-based traceability systems is the implementation of on-chain and off-chain data storage mechanisms. The choice between on-chain and off-chain data storage involves several trade-offs affecting auditability and traceability. On-chain storage means writing data directly to the blockchain, which maximizes integrity and transparency but incurs high costs and limited throughput [89].

  In contrast, off-chain storage (keeping data off the ledger and recording only hashes or references on-chain) enhances efficiency and scalability. However, it requires trusting external systems or additional proofs. Key trade-offs include preserving hash keys (cryptographic digests) on the blockchain while retaining comprehensive data off-chain. This strategy reduces blockchain storage expenditures and improves privacy, while maintaining data integrity [57]. Many systems use hybrid architectures to balance these concerns, keeping only essential proofs on-chain and bulk data off-chain.

TABLE VII. CONSENSUS ALGORITHMS VS ACCOUNTABILITY

Consensus Algo.	Accountability Level	Validators Identified	Misbehavior Traceable	Punishment Supported
PoW.	Low.	Pseudonymous miners.	Very limited.	Not natively supported.
PoS.	Medium.	Validators are known.	Depend on implementa-tion	Often slashing-based.
PBFT.	High.	Known validator set.	Full message logs & signatures.	Rule-based punishment.
BDLS.	Very High.	Known validators.	Threshold signatures prove votes.	Strong accountability.
Raft.	Low-Medium.	Known leaders and replicas.	Faults are traceable but not byzantine.	No punishment mechanism.
HotStuff.	High.	Known validators.	Signed voting rounds.	Often slashing-based.
Longest Chain.	Very Low.	Pseudonymous miners.	No identity or blame.	No deterrence/punishment.

- **Smart Contract-Based Audit Log Systems:** Smart contracts may be employed to implement consensus algorithms and mitigate collusion attacks within audit log systems. For example, a blockchain-based audit log system is capable of generating sub-Non-Fungible Tokens (sub-NFTs) for each log file, securely storing these tokens on the blockchain as proof of integrity. This approach not only conserves blockchain storage space but also guarantees data integrity within a generalized threat model in which specific nodes may be deemed untrustworthy [46].
- **Formal Verification for Smart Contract Security:** To mitigate security vulnerabilities in smart contracts, formal verification techniques can be employed to enhance security. These methodologies, which are highly effective in identifying vulnerabilities and logical inconsistencies in smart contracts, amalgamate static analysis, formal verification, and analog execution. For instance, a security audit methodology predicated on formal verification can uncover prevalent vulnerabilities such as reentrancy and integer overflow, thereby enhancing the security of smart contracts prior to their deployment [90].
- **Hash Functions for Data Integrity:** Hash functions are extensively employed within blockchain architectures to ascertain the integrity of data. For instance, Merkle trees facilitate the generation of a root hash that encapsulates the integrity of a given dataset. This root hash may be recorded on the blockchain, thereby enabling the efficient validation of data integrity without necessitating the storage of the entire dataset on-chain [77].
- **Consensus Algorithm:** The architecture of a consensus algorithm significantly influences the degree of accountability that can be achieved within a blockchain framework. Protocols that employ robust cryptographic voting mechanisms, Byzantine Fault Tolerance (BFT) consensus, and auditable logging mechanisms provide enhanced levels of accountability. In contrast, systems such as Proof-of-Work generally exhibit diminished traceability concerning responsibility. Table VI illustrates how consensus algorithms affect accountability.

  In [69], the BDLS (Byzantine DLS) consensus protocol improves accountability in blockchain systems by utilizing cryptographic voting mechanisms that incorporate threshold signatures. This method ensures that each node's participation in the consensus process is both verifiable and secure. If a node attempts to propose conflicting blocks or cast multiple votes, such misbehavior can be identified and proven through signed cryptographic evidence. Additionally, the protocol maintains comprehensive logs of all votes and proposals, allowing the system to detect and trace malicious actions reliably. This traceability supports the enforcement of governance rules, including the possibility of penalizing or removing nodes that violate the integrity of the consensus. Table VII categorizes various blockchain consensus algorithms based on their level of accountability. BDLS, PBFT, HotStuff, and Tendermint are classified as having strong accountability, as they incorporate digital signatures, maintain detailed records of validator votes, and support mechanisms for penalizing misbehavior. In contrast, Raft and Proof-of-Stake (PoS) protocols provide only partial accountability, relying on additional system logic or external enforcement methods such as slashing contracts to deter or respond to faults. At the lowest end of the spectrum, Proof-of-Work (PoW) based blockchains are considered to have minimal accountability, as validator identities are typically anonymous and detecting or proving malicious behavior is inherently difficult or infeasible.

- **Chameleon Hashes for Privacy-Preserving Auditing:** Chameleon hashes constitute a category of cryptographic primitives that facilitate meticulous data modification and access, all the while safeguarding user privacy. These

hashes are employed within redactable blockchains to permit auditing and tracing endeavors without jeopardizing user confidentiality. In [36], the authors propose the Redact4Trace solution, which utilizes chameleon hashes to maintain user privacy while ensuring the integrity of audit logs.

- **Homomorphic Verifiable Tags for Batch Verification:** This approach is used in data auditing frameworks to facilitate batch verification of data integrity without the need for third-party auditors [54]. These tags enable the verification of multiple data blocks in a single operation, thereby reducing computational and communication costs. This methodology proves especially beneficial in multi-cloud storage environments, where data is disseminated across multiple service providers.

TABLE VIII. SUMMARY OF ACCESS CONTROL MECHANISMS

Ref.	Method	Attribute
[57]	On-chain and off-chain data storage.	Achieves a harmonious integration of scalability and privacy.
[46]	Smart contract-based audit log systems.	Utilizes sub-NFTs and decentralized file systems.
[55, 60]	Formal verification for smart contracts.	Identifies weaknesses inconsistencies within smart contracts.
[36]	Chameleon hashes for privacy-preserving auditing.	Safeguards the confidentiality of users.
[54]	Homomorphic verifiable tags for batch verification.	Facilitates economical batch verification of data integrity.
[53]	Deep learning for audit data traceability.	Augments the traceability and validation of audit information.
[46]	Distributed file systems for data integrity.	Guarantees the accessibility and authenticity of off-chain information.

Numerous advanced approaches have been proposed to improve the auditability and traceability of blockchain systems. These encompass the application of deep learning, distributed file systems, and automated verification models. Deep learning methodologies can be combined with blockchain technology to enhance the traceability and verification of audit data. For example, a deep learning-based system can perform data mining and clustering to identify patterns and anomalies within audit data. This approach improves the efficiency and effectiveness of the auditing process by taking advantage of the capabilities of deep learning algorithms [53].

On the other hand, distributed file systems can be integrated with blockchain technology to ensure the integrity of data stored off-chain. For instance, in a blockchain-enabled auditing log system, log files can be stored in a distributed file system. This setup addresses the risk of a single point of failure and ensures the continuous availability of auditing data [46].

Furthermore, automated verification models, exemplified by the AUDITEM framework, utilize smart contracts in conjunction with distributed file systems to store attributes related to integrity verification. These models significantly enhance the authenticity of data certificates while providing user-friendly interfaces for customized verification processes. The AUDITEM framework has demonstrated considerable efficiency and practicality in fulfilling diverse business demands for data integrity verification [55]. Table VIII presents a comparative analysis of principal techniques for the implementation of audibility and traceability within blockchain systems.

6.2 RQ2: How Do Smart Contracts Contribute to Enforcing Accountability in Decentralized Systems?

When designing a blockchain system, it is essential to have a programming language specifically designed for writing smart contracts. Smart contracts symbolize the services that users create within that system [91]. Numerous programming languages facilitate such a thing, but Solidity is the most appropriate programming language to create intelligent contracts [92]. These characteristics render them exceptionally appropriate for securing accountability within decentralized systems. In the following discussion, we will examine the technical mechanisms that facilitate accountability and the challenges accompanying their implementation.

- Automated Execution: Smart contracts facilitate the automatic execution of predetermined stipulations upon the fulfillment of specific criteria, thereby obviating the necessity for intermediaries. This automation mitigates the likelihood of human error and nefarious interference, thereby ensuring that actions are executed in a consistent and dependable manner [79], [73]. For example, within the realm of public procurement, smart contracts possess the capability to automate the bidding processes, supplier accreditation, and delivery confirmation, thereby diminishing the potential for corruption and reinforcing accountability [79].

- Transparency: The transparency inherent in smart contracts constitutes a fundamental principle of accountability. Every transaction and execution is documented on a blockchain, resulting in a ledger that is both immutable and publicly accessible. This transparency enables stakeholders to conduct audits and verify the execution of smart contracts, thereby ensuring that all actions are traceable and observable [73], [93].
- Immutability: The immutable quality of blockchain technology ensures that the regulations and transactions controlled by smart contracts are immune to retroactive modifications. This element is critical for enhancing trust and accountability, as it prevents any revisions to the agreement or its execution [79]. Nevertheless, challenges persist, including the possibility of coding errors that may result in unforeseen consequences, and the absence of legal recognition could impede their enforceability. Furthermore, while transparency mitigates information asymmetries, it may inadvertently reveal sensitive information. These considerations underscore the necessity for meticulous design and the thoughtful integration of legal frameworks to harness the potential of smart contracts in governance fully [93].

Despite their inherent potential, smart contracts face numerous challenges and constraints that may hinder their effectiveness in ensuring accountability.

Bugs and vulnerabilities pose significant challenges that can undermine the accountability of smart contracts, allowing malicious actors to exploit the system or misappropriate funds [94]. Moreover, smart contracts often lack legal recognition in many jurisdictions, which can lead to ambiguity and potential legal disputes. This absence of formal recognition may deter the adoption of smart contracts for accountability, as stakeholders might be wary of relying on a technology that lacks strong legal support [95].

In terms of cross-chain applications, the functionality of smart contracts often encounters challenges when attempting to interact with various blockchain platforms, thereby constraining their overall efficacy [96]. Cross-chain interoperability is essential for comprehensive accountability across heterogeneous blockchain networks, since fragmentation has created isolated “data and value silos” that constrain unified oversight [97]. For example, Wei et al. propose BEAIV, a blockchain-enabled cross-chain audit scheme that detects data tampering and traces responsibility for dishonest behavior across chains [98]. In general, enhanced interoperability is recognized to improve transparency and accountability of data management across platforms, enabling more effective cross-chain auditing and oversight, blockchain observatory [99]. Furthermore, the absence of uniformity in smart contract languages and platforms significantly obstructs interoperability [78]. Additionally, the issue of scalability represents a critical obstacle confronting smart contracts. The constrained transaction processing capacity of blockchain networks, exemplified by Ethereum, obstructs their implementation in extensive applications. Therefore, the limitations of current blockchain systems can be summarized as follows:

1. **Transaction throughput:** Blockchain frameworks such as Ethereum exhibit constraints in transaction throughput, rendering them inadequate for applications necessitating real-time processing [100].
2. **State Channel Latency:** State channels, which serve to augment scalability, frequently experience significant collateral requirements and initialization latency [101], [102].

In addition, the presence of coding errors within smart contracts poses a significant concern due to the immutable nature of blockchain technology. Once these smart contracts are deployed, they cannot be altered, making it imperative to verify their accuracy before deployment. Empirical studies have demonstrated that even minor coding mistakes can result in significant financial detriment, as exemplified by incidents such as the DAO hack and the Parity wallet vulnerability [103], [104]. The discrepancies in coding within smart contracts frequently arise from:

1. Reentrancy Attacks: These incidents transpire when a malicious actor takes advantage of a contract’s fallback function to deplete financial resources, as illustrated in the DAO breach [103], [105].
2. The Deployment of Unsecured Libraries: Arrangements that rely on unsecured libraries or external dependencies show significant vulnerability to numerous attack vectors.
3. Utilization of Vulnerable Libraries: Configurations that depend on unsecured libraries or external dependencies exhibit considerable susceptibility to a variety of attack vectors [106], [107].
4. Integer Overflow/Underflow: Such vulnerabilities may result in unforeseen behaviors, including unintended monetary transfers [108].

In order to rectify coding inaccuracies, scholars have suggested an array of detection and remediation methodologies: • Formal Verification: Methodologies, including formal verification, possess the capacity to rigorously demonstrate the correctness of smart contracts through mathematical proofs [78].

- Fuzz Testing: Hybrid dynamic analysis methodologies, encompassing console execution alongside fuzzing techniques, have demonstrated efficacy in identifying intricate vulnerabilities within smart contracts [109].
- Machine Learning: Various machine learning paradigms, such as graph neural networks and multi-task learning, have been employed to identify vulnerabilities within smart contracts [110], [111].

TABLE IX. COMPARISON OF PRINCIPAL OBSTACLES AND REMEDIAL STRATEGIES

Ref.	Challenge	Description	Solution
[63, 64]	Coding errors.	Reentrancy attacks, integer overflow, and unsecured libraries lead to vulnerabilities.	Formal verification, fuzz testing, and machine learning models.
[47, 60]	Scalability issues.	Limited transaction throughput and state channel latency hinder scalability.	State channel protocols, credit-note systems, and off-chain transactions.
[33, 60]	Interoperability.	Lack of standardization and cross-chain compatibility limit utility.	Cross-chain protocols and universal composability frameworks.
[42, 47]	Accountability.	Lack of auditability and decentralized nature complicate accountability.	Trusted delegation of tasks and real-time monitoring.

In short, Table IX summarizes the key challenges. Smart contracts encounter considerable technical obstacles in domains such as programming inaccuracies, scalability limitations, interoperability issues, and accountability concerns. Tackling these obstacles necessitates a multidisciplinary methodology, integrating advancements in formal verification, machine learning, and protocol architecture. Through the utilization of these technologies, scholars and developers can formulate more resilient, scalable, and interoperable smart contracts, thereby ultimately augmenting their acceptance and trust within the blockchain ecosystem.

6.3 RQ3: What Role Does Access Control Play in Strengthening Trust and Responsibility in Blockchain-Enabled Infrastructures?

In response to the research question on how blockchain enhances access control and identity management, the literature demonstrates that blockchain technology introduces decentralized, secure, and transparent mechanisms for managing access rights. Key access control models identified include RBAC and ABAC, both of which have been adapted to operate within blockchain environments. Table X presents a synthesized overview of the blockchain execution services examined in the reviewed literature.

These models are integrated into identity management frameworks to ensure that only authorized users can interact with specific data or services. Reviews of studies distinguish between permissioned and permissionless blockchains, highlighting how access policies and identity verification processes vary according to the level of decentralization and trust assumptions [62].

Technical implementations across various platforms show that blockchain-enabled access control not only mitigates a single point of failure but also provides immutable logs for accountability. These findings collectively emphasize the growing role of blockchain in transforming traditional access control systems into more robust and transparent architectures.

6.3.1. Role-Based Access Control in Blockchains

RBAC is a traditional approach to managing access to resources based on roles assigned to users. In blockchain systems, RBAC can be implemented to provide a structured and scalable access control mechanism. The integration of RBAC with blockchain technology offers several advantages, including transparency, immutability, and decentralized governance.

6.3.2. Mechanisms of RBAC in Blockchains

Role Specification and Hierarchical Framework: In decentralized blockchain-centric RBAC systems, roles are delineated in accordance with organizational frameworks, and hierarchies are instituted to regulate access authorizations. For instance, administrative roles possess the capacity to bestow or retract permissions to individuals, thereby ensuring that access regulation is both fluid and responsive to organizational transformations [112].

6.4 Oracle Problem and Data Validation in Ingress

The blockchain "oracle problem" highlights that blockchains cannot inherently verify external data and must instead rely on oracles – trusted bridges to off-chain sources – which inevitably reintroduce trust assumptions and single points of failure [114]. This issue is especially critical for Ingress, which aggregates heterogeneous off-chain inputs (e.g., IoT sensor readings, financial feeds, electronic health records) before writing them to one or more blockchains. If an IoT sensor is faulty [115], or malicious, or if financial or medical data are fraudulent or erroneous, those inaccuracies would be permanently recorded on-chain. Because blockchains are immutable, any such incorrect data cannot be deleted or corrected afterward [116].

TABLE X. A SUMMARY OF BLOCKCHAIN EXECUTION SERVICES

Ref.	Smart Contract	Access Control
[57]	Yes	No
[63]	No	No
[59]	No	No
[48]	No	Yes
[34, 45, 48]	No	No
[33, 53]	Yes	Yes
[46]	Yes	No
[35, 41, 56]	No	Yes
[38, 65]	Yes	No
[113]	No	No
[44]	Yes	No
[35, 38, 44, 45, 59, 62]	Yes	No

To prevent this, Ingress performs rigorous upstream validation: it cross-checks incoming data against multiple independent sources, requires cryptographic proofs of authenticity (for example, digital signatures or zero-knowledge proofs [116], and applies automated anomaly-detection algorithms (with human review for critical cases). These measures ensure that only verified, trustworthy data is committed to the immutable ledger, addressing the oracle problem at the ingestion point.

6.5 RQ4: What Are the Strengths and Limitations of Current Models Combining These Mechanisms for Accountability Enhancement?

- **Strength:** By capturing all transactions and data interactions, the incorporation of blockchain technology creates a decentralized ledger that improves accountability and transparency, allowing users to audit it [34]. Furthermore, mechanisms such as digital signatures and commitment schemes are used to guarantee public accountability, facilitating the identification of those who make modifications in the event of malicious alterations [54]. The proposed models can effectively prevent malicious behavior from both third parties and users, thereby improving data integrity and trustworthiness [55].
- **Limitations:** Existing models face scalability challenges, especially in multi-cloud settings, where the auditing process may result in considerable computational and communication burdens [62]. Additionally, concerns exist regarding data recoverability and potential security issues arising from system complexity. The reliance on untrusted entities, such as cloud service providers, poses risks of data loss or manipulation, which can undermine the overall accountability framework [46]. To address the scalability concern, we suggest moving to a multi-layer or partitioned blockchain architecture. For example, using sharding or DAG-based ledgers can parallelize transaction processing (each shard handles only a subset of data) [117]. Likewise, layer-2 or sidechain solutions (e.g., state channels or rollups) can batch audit transactions off the main chain to significantly reduce on-chain burden. To improve data recoverability, we recommend distributed redundancy. For instance, erasure-coding data across multiple clouds

ensures that the original data can be reconstructed even if some pieces are lost. Periodically anchoring backup or snapshot hashes in the blockchain creates an immutable audit trail for recovery operations, making any tampering or data loss evident. In practice, requiring consensus or threshold signatures from several clouds (and using cryptographic proofs, such as proofs-of-retrievability or TPM/TEE validation) ensures that data integrity is maintained even if one provider is compromised. These improvements—parallelized ledgers, resilient multi-cloud storage, and fully distributed verification—help solve the main issues we identified and make our system more accountable.

7. DISCUSSIONS

7.1 Identified Gaps

The formulation of novel systems or the incorporation of blockchain technology into established frameworks within different institutions poses numerous challenges, several of which are uniquely pertinent to the specific domain of application. While a wealth of research focuses on blockchain's role in auditing and traceability, several crucial gaps remain that hinder the advancement and broader application of these studies.

TABLE XI. RESEARCH GAPS AND THEIR RELATION TO THE RESEARCH QUESTION

Identified gaps	Relation to RQs
First gap	RQ1, RQ2
Second gap	RQ1, RQ2, RQ3, RQ4
Third gap	RQ1

TABLE XII. A SUMMARY OF BLOCKCHAIN PLATFORM

Ref.	Ethereum	Bitcoin	Hyperledger Fabric	NEO	IOTA	Tron
[57]	Yes	No	No	No	No	No
[63]	Yes	No	No	No	No	No
[59]	Yes	No	Yes	Yes	No	No
[48]	No	No	No	No	Yes	No
[34, 45, 48]	No	No	No	No	No	Yes
[33, 53]	No	No	No	No	No	Yes
[46]	No	No	Yes	No	No	No
[35, 41, 56]	No	No	No	Yes	No	No
[38, 65]	Yes	No	No	No	No	Yes
[113]	Yes	No	No	Yes	No	No
[44]	No	No	Yes	No	No	No
[35, 38, 44, 45, 59, 62]	No	Yes	Yes	No	No	No

First, while auditability and traceability get a lot of attention, there's a significant lack of accountability mechanisms, especially in decentralized settings. The lack of such an element detracts from the enforceability of obligations and renders the governance of permissionless or semi-permissioned systems more complex [57]. In open blockchain systems, the concept of 'public accountability' is understood to mean that any party—including unauthorized users—who alters a transaction can be identified and held responsible. This feature implies that accountability mechanisms are recognized in principle, but their implementation or effectiveness is limited. This reflects the gap in current practice.

Second, although the concept of data traceability is a prevalent focus within the literature, the subject of secure and privacy-preserving data sharing is still predominantly insufficiently examined. A limited number of studies address the complexities

associated with facilitating multi-party collaboration over sensitive datasets in a way that concurrently upholds both transparency and confidentiality, particularly in critical domains such as healthcare and finance. While the core gap points to insufficient examination of secure and privacy-preserving multi-party data sharing that balances transparency and confidentiality, several papers are actively working on various facets of this challenge. They propose blockchain-based solutions, privacy-enhancing technologies, and frameworks that aim to provide secure, transparent, and auditable data exchange, particularly in sensitive domains like healthcare and finance [51], [48], [55].

Third, the application of federated learning alongside blockchain technology remains in a nascent stage of development. While this methodology shows promise for facilitating distributed audit intelligence without infringing on data sovereignty, existing research provides scant architectural perspectives and evaluative frameworks. Moreover, the utilization of smart contracts is frequently limited to basic transactional verification rather than the thorough enforcement of logic pertinent to audit and compliance responsibilities. This limitation constrains the efficacy of blockchain technology within fluid regulatory frameworks, wherein the execution of adaptable and verifiable logic is of paramount importance. Ultimately, applications specific to particular domains, including supply chain transparency, public health infrastructure, and intellectual property authentication, continue to be inadequately addressed within the existing scholarly literature. Most of the proposed frameworks lack complete performance validation and proof of real-world application domains, which eventually results in the restricted practicality of the theoretical models. Thus, as proven, a need for further research exists in the form of a cohesive approach to accountability, interoperability, data governance, and context-aware audit systems. This is primarily done through implementing blockchain and related technologies, including AI and federated learning, to develop comprehensive and scalable privacy-aware audit frameworks [48].

7.2 What Role Does the Type of Platform Play to Enhancing Blockchain-Based Accountability Mechanisms

The type of blockchain has a significant impact on how accountability mechanisms are applied and strengthened within a blockchain. A public blockchain (e.g., Ethereum, Bitcoin) aims to provide maximum transparency and traceability, while a private blockchain (E.g., Hyperledger Fabric) aims to provide controlled, auditable accountability in a trusted environment. Hybrid models serve both requirements. Table XII summarizes the platform used in the reviewed articles.

7.3 Role of Machine Learning for Efficient Blockchain Accountability

Binary neural networks (BNNs) and Tsetlin mechanisms are effective for on-chain anomaly and fraud detection as well as compliance tasks because of their low computational requirements. A lightweight BNN implemented on a Cortex M4 microcontroller has been used to detect electrocardiogram (ECG) anomalies within a blockchain-enabled health monitoring system [18]. AI-driven detection techniques can significantly enhance trust and resilience in networked systems. For instance, Al-Ibraheemi et al. developed an intrusion-detection system for software-defined networks that combines graph convolutional networks with deep reinforcement learning; their approach achieved 93.8 percent detection accuracy and "establishes the groundwork for resilient infrastructure" [20].

In our work, we extend this idea to blockchain ecosystems by embedding lightweight ML models to improve accountability. For example, a BNN on a Cortex-M4 microcontroller was used to detect cardiac anomalies in a blockchain-enabled health monitoring framework [18], and convolutional Tsetlin Machines have been applied to create CTMBIDS, a DDoS detector noted for its "lightweight nature" (very low memory use and fully interpretable rules) [19]. Deploying such efficient, logic-based detectors at the network edge or among blockchain validators enables continuous real-time auditing of transactions with minimal overhead. Blockchain systems also depend on strong cryptography for security. Advanced Encryption Standard (AES) is widely used, and studies of AES performance in contexts like voice cryptography emphasize the need to balance efficiency and security in resource-constrained environments [21]. Complementing conventional ciphers, new lightweight cryptosystems have been proposed for IoT and smart cities. For example, Hazzaa et al. introduced a lightweight encryption algorithm using dual XOR S-boxes that reduces execution time and power consumption by about 33 percent compared to standard AES while maintaining security [22]. These approaches demonstrate that cryptographic efficiency can be improved without sacrificing security – a key requirement for scalable, low-overhead accountability in blockchain-based infrastructure.

7.4 Recommendations and Future Research Directions

- **Strengthen Traceability Systems:** Traceability systems have to be strengthened in the sense that information not only has to be traceable, but also respect for privacy based on GDPR and similar data protection laws to responsibly manage sensitive information [57].

- **Leverage the Advanced Technologies:** Utilization of other technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) can improve the efficiency of traceability and auditability systems to collect and analyze real-time data, thus improving the quality of decisions by making them analytics-driven.
- **Consideration of Data Ownership and Liability:** Further research would unite the debate about accountability and liability when mistakes occur in traceability data within public blockchains [52].
- **Implement Strong Access Control Mechanisms:** Researching robust access control mechanisms, such as role-based access control, can enhance the security of traceability data and prevent unauthorized access [47],[118].

8. CONCLUSION

The current landscape of blockchain-based accountability mechanisms reveals a strong reliance on the inherent immutability of blockchain technology to ensure auditability and traceability. These characteristics enable the creation of tamper-evident records that enhance transparency and foster trust among stakeholders across various domains. The integration of smart contracts within these frameworks further reinforces accountability by automating the enforcement of predefined rules and standards, thereby minimizing the risk of human error and fraud while ensuring consistent compliance in decentralized systems. For example, blockchain applications in the accounting of carbon emissions have demonstrated notable improvements in the accuracy and transparency of ESG reporting. Smart contracts also play a pivotal role in traceability by automating data verification and improving collaboration across supply chains. Meanwhile, access control mechanisms are crucial for maintaining the integrity and confidentiality of sensitive information.

In addition, a lightweight ML algorithm such as BNNs and the Tsetlin Machine has a significant role in enhancing blockchain accountability. Specifically, in applications that address a fraud detection, anomaly detection, and compliance tracking, particularly within resource-constrained environments.

By restricting access to authorized users, these mechanisms mitigate security risks and bolster trust within blockchain-enabled infrastructures. Despite these advancements, challenges persist. The implementation of blockchain-based accountability mechanisms often incurs high operational costs and computational demands, particularly when integrated with emerging technologies such as machine learning. Furthermore, the effectiveness of such systems remains contingent upon the development of robust access control strategies to safeguard against unauthorized actions. In summary, while current approaches offer significant benefits in terms of data integrity, transparency, and automated compliance, future research should focus on optimizing these mechanisms for scalability, cost-efficiency, and enhanced security to fully realize the potential of blockchain in accountability systems.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Cryptography Mailing list at https://metzdowd.com*, 03 2009.
[2] F. Casino *et al.*, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.
[3] T. Aste *et al.*, “Blockchain technologies: The foreseeable impact on society and industry,” *Computer*, vol. 50, pp. 18–28, 01 2017.
[4] A. Akram *et al.*, “Trust, privacy and transparency with block-chain technology in logistics,” 09 2018.
[5] R. Batubara *et al.*, “Unraveling transparency and accountability in blockchain,” ser. ACM International Conference Proceeding Series. ACM, 2019, pp. 204–213.
[6] S. B *et al.*, “Blockchain industry 5.0: Next generation smart contract and decentralized application platform,” in *IEEE ICSES*, 2022, pp. 1–8.
[7] M. Subhy *et al.*, “Blockchain technology and internet of things: review, challenge and security concern,” *IJECE*, vol. 13, p. 718, 02 2023.
[8] Z. Cui *et al.*, “A hybrid blockchain-based identity authentication scheme for multi-wsn,” *IEEE TSC*, vol. 13, no. 2, pp. 241–251, 2020.
[9] S. Baker and A. Nori, “A secure proof of work to enhance scalability and transaction speed in blockchain technology for iot,” 01 2023, p. 040008.
[10] A. Alghuried *et al.*, “Blockchain security and privacy: Threats, challenges, applications, and tools,” *Distrib. Ledger Technol.*, Feb 2025.
[11] T. Savelyeva *et al.*, “Blockchain technology for sustainable education,” *BJET*, vol. 53, no. 6, pp. 1591–1604, 2022.
[12] N. Sultan *et al.*, “Container-based virtualization for blockchain technology: A survey,” *JJCIT*, vol. 9, p. 1, 09 2023.

[13] N. Z. Tawfeeq, W. S. Abed, and O. G. Ghazal, "A semantic model of morphological information retrieval: A comparative accumulative analysis," in *2020 2nd Annual International Conference on Information and Sciences (AiCIS)*, 2020, pp. 1–6.
[14] N. A. Sultan *et al.*, "Blockchain-based framework for secure monitoring of vehicles traffic flow system," in *IEEE COMNETSAT*, 2023, p. 226.
[15] U. Rahardja *et al.*, "Blockchain application in educational certificates and verification compliant with general data protection regulations," in *10th CITSM*, 2022, pp. 1–7.
[16] J. M. Song *et al.*, "Applications of blockchain to improve supply chain traceability," *Procedia Computer Science*, vol. 162, pp. 119–122, 2019.
[17] O. Ghazal *et al.*, "Tinyml: Applications, algorithms, hardware/software co-design and implementations," in *Smart and Connected Healthcare*. Springer, 2025, in Press.
[18] B. Borah *et al.*, "Blockchain-enabled heartcare framework for cardiovascular disease diagnosis in devices with constrained resources," *IEEE Transactions on Services Computing*, vol. PP, pp. 1–14, 11 2024.
[19] R. Jafari Gohari *et al.*, "Ctmbids: Convolutional tsetlin machine based intrusion detection system for ddos attacks in an sdn environment," *arXiv preprint arXiv:2409.03544*, 2024, arXiv:2409.03544v1.
[20] F. Alibrahimi *et al.*, "Intrusion detection in software-defined networks: Leveraging deep reinforcement learning with graph convolutional networks for resilient infrastructure," *Fusion Practice and Applications*, vol. 15, pp. 78–87, 02 2024.
[21] F. Hazzaa *et al.*, "Performance analysis of advanced encryption standards for voice cryptography with multiple patterns," *International Journal of Safety and Security Engineering*, vol. 14, no. 5, pp. 1439–1446, 2024.
[22] F. Hazzaa *et al.*, "A new lightweight cryptosystem for IoT in smart city environments," *Mesopotamian Journal of CyberSecurity*, vol. 4, pp. 174–186, Oct. 2024.
[23] M. Borrego *et al.*, "Systematic literature reviews in engineering education and other developing interdisciplinary fields," *JEE*, vol. 103, no. 1, pp. 45–76, 2014.
[24] M. Moher, "Preferred reporting items for systematic reviews and meta-analyses: The prisma statement," *Annals of Internal Medicine*, vol. 151, no. 4, pp. 264–269, 2009.
[25] H. Han *et al.*, "Accounting and auditing with blockchain technology and artificial intelligence: A literature review," *IJAIS*, vol. 48, p. 100598, 2023.
[26] A. R. Sai *et al.*, "Taxonomy of centralization in public blockchain systems: A systematic literature review," *Information Processing & Management*, vol. 58, no. 4, p. 102584, 2021.
[27] E. Tan *et al.*, "Blockchain governance in the public sector: A conceptual framework for public management," *Government Information Quarterly*, vol. 39, no. 1, p. 101625, 2022.
[28] A. Rustemi *et al.*, "A systematic literature review on blockchain-based systems for academic certificate verification," *IEEE Access*, vol. 11, pp. 64679–64696, 2023.
[29] M. N. M. Bhutta *et al.*, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.
[30] T. K. Dahariya *et al.*, "Enhancing livestock supply chains with blockchain traceability from source to market: A survey," in *IESIC*, 2025.
[31] S. Sheela *et al.*, "Navigating the future: Blockchain's impact on accounting and auditing practices," *Sustainability*, vol. 15, no. 24, 2023.
[32] A. T. Polcumpally *et al.*, "Blockchain governance and trust: A multi-sector thematic systematic review and exploration of future research directions," *Heliyon*, vol. 10, no. 12, p. e32975, 2024.
[33] S. J. Shabu *et al.*, "Enhanced blockchain-based decentralized public auditing for cloud storage," in *ICOECA*, 2024, pp. 107–111.
[34] G. Indiravathi *et al.*, "Enhancing data privacy and accountability in smart grids with blockchain technology," in *ICEECT*, vol. 1, 2024, pp. 1–6.
[35] P. Zhu *et al.*, "Using blockchain technology to enhance the traceability of original achievements," *IEEE TEM*, vol. 70, no. 5, 2023.
[36] J. Hu *et al.*, "Redact4trace: A solution for auditing the data and tracing the users in the redactable blockchain," *Computer Networks*, vol. 245, p. 110360, 2024.
[37] I. P. S. Setiawan *et al.*, "Enhancing security, privacy, and traceability in indonesia's national health insurance claims process using blockchain technology," in *ICoABCD*, 2023, pp. 77–82.
[38] G. Jeong *et al.*, "Azeroth: Auditable zero-knowledge transactions in smart contracts," *IEEE Access*, vol. 11, pp. 56463–56480, 2023.

[39] A. Alamsyah *et al.*, "Enhancing privacy and traceability of public health insurance claim system using blockchain technology," *Frontiers in Blockchain*, vol. 8, p. 1474434, 2025.
[40] Y. Xu *et al.*, "Pirb: Privacy-preserving identity-based redactable blockchains with accountability," *Electronics*, vol. 12, no. 18, 2023.
[41] A. K. Bapatla *et al.*, "Pharmachain 3.0: Efficient tracking and tracing of drugs in pharmaceutical supply chain using blockchain integrated product serialization mechanism," *SN Computer Science*, vol. 5, no. 1, p. 149, 2024.
[42] M. Banu *et al.*, "A machine learning approach for enhanced security using blockchain in finance auditing services," in *15th ICCCNT*, 2024.
[43] V. Sharma *et al.*, "Enhancing traceability in agricultural supply chain using blockchain technology," *IJIEEB*, vol. 16, no. 3, pp. 11–21, 2024.
[44] Q. Tang, "Towards using blockchain technology to prevent diploma fraud," *IEEE Access*, vol. 9, pp. 168678–168688, 2021.
[45] A. Guayasamín *et al.*, "Blockchain-enhanced e-ticket distribution system to effective transactions, validation, and audits," in *8th CSNet*, 2024.
[46] Z. Liu *et al.*, "A secure and reliable blockchain-based audit log system," in *IEEE ICC*, 2024, pp. 2010–2015.
[47] E. M. Alotaibi *et al.*, "Blockchain-driven carbon accountability in supply chains," *Sustainability*, vol. 16, no. 24, 2024.
[48] H. Zeng *et al.*, "A federated learning framework with blockchain-based auditable participant selection," *CMC*, vol. 79, no. 3, pp. 5125–5142, 2024.
[49] C.-L. Chen *et al.*, "Constructing a secure charity nft auction platform using fisco bcos blockchain for enhancing transparency and traceability," *IEEE Access*, vol. 12, pp. 36924–36941, 2024.
[50] S. Y. A. Zaidi *et al.*, "An attribute-based access control for iot using blockchain and smart contracts," *Sustainability*, vol. 13, no. 19, 2021.
[51] Y. Wang *et al.*, "Spds: A secure and auditable private data sharing scheme for smart grid based on blockchain," *IEEE Trans. on Industrial Informatics*, vol. 17, no. 11, pp. 7688–7699, 2021.
[52] U. V *et al.*, "Enhancing health product traceability on the blockchain: A novel approach for supply chain management inspection to ai," *EAI Endorsed Transactions on Pervasive Health and Technology*, 03 2024.
[53] Y. Zhao, "Audit data traceability and verification system based on blockchain technology and deep learning," in *TELEPE*, 2024, pp. 77–82.
[54] C. Zhang *et al.*, "A blockchain-based multi-cloud storage data auditing scheme to locate faults," *IEEE TCC*, vol. 10, no. 4, 2022.
[55] Z. Shi *et al.*, "Auditem: Toward an automated and efficient data integrity verification model using blockchain," 2022. [Online]. Available: https://arxiv.org/abs/2207.00370
[56] R. Hortelano-Haro *et al.*, "Harnessing blockchain technology to enhance trust and traceability in wine trading among wineries," *IT Professional*, vol. 26, no. 4, pp. 80–88, 2024.
[57] M. J. Fernández-Iglesias *et al.*, "Efficient traceability systems with smart contracts: Balancing on-chain and off-chain data storage for enhanced scalability and privacy," *Applied Sciences*, vol. 14, no. 23, 2024.
[58] R. Konapure *et al.*, "Traceability and verification to prevent counterfeit drugs: A secure, efficient pharma supply chain with iot-enabled blockchain and smart contracts," *IJECE*, vol. 12, no. 1, pp. 33–43, 2025.
[59] V. Mothukuri *et al.*, "Blockhdfs: Blockchain-integrated hadoop distributed file system for secure provenance traceability," *Blockchain: Research and Applications*, vol. 2, no. 4, p. 100032, 2021.
[60] S. Xiao *et al.*, "Blockchain-based framework for secure sharing of cross-border trade data," *CMC*, vol. 83, no. 2, pp. 2351–2373, 2025.
[61] W. Serrano, "Verification and validation for data marketplaces via a blockchain and smart contracts," *Blockchain: Research and Applications*, vol. 3, no. 4, p. 100100, 2022.
[62] Y. Tian *et al.*, "Accountable fine-grained blockchain rewriting in the permissionless setting," 04 2021.
[63] E. Yigit and T. Dag, "Improving supply chain management processes using smart contracts in the ethereum network written in solidity," *Applied Sciences*, vol. 14, no. 11, 2024.
[64] S. Peng *et al.*, "Enhancing cross-border data sharing in blockchain networks: A compliance-centric approach ensuring anonymity and traceability," in *3rd CCSB*, 2023, pp. 200–204.
[65] N. B. Junaidi *et al.*, "Design and implementation of blockchain-based smart contracts for enhancing ancillary services management in electricity markets," in *IEEE PECon*, 2024, pp. 76–81.
[66] W. Cram *et al.*, "(re)considering the concept of literature review reproducibility," *JAIS*, vol. 21, 09 2020.
[67] S. Dhall *et al.*, "Blockchain-based framework for reducing fake or vicious news spread on social media/messaging platforms," *Association for Computing Machinery*, vol. 21, no. 1, Nov. 2021.

[68] Y. Chen *et al.*, "Towards trusted social networks with blockchain technology," 2018. [Online]. Available: https://arxiv.org/abs/1801.02796 [69] A. Al Salih *et al.*, "Bdls as a blockchain finality gadget: Improving byzantine fault tolerance in hyperledger fabric," *IEEE Access*, 2024.
[70] M. Memon *et al.*, "Blockchain beyond bitcoin: Blockchain technology challenges and real-world applications," in *iCCECE*, 2018, pp. 29–34.
[71] P. Kochovski *et al.*, "Trust management in a blockchain based fog computing platform with trustless smart oracles," *FGCS*, vol. 101, pp. 747–759, 2019.
[72] D. Di Francesco Maesa *et al.*, "A blockchain based approach for the definition of auditable access control systems," *Computers Security*, vol. 84, pp. 93–119, 2019.
[73] K. Nabben *et al.*, "Accountability protocols? on-chain dynamics in blockchain governance," *IPR*, vol. 13, no. 4, pp. 1–22, 2024.
[74] L. Hughes *et al.*, "Understanding accountability in blockchain systems," *Accounting, Auditing Accountability Journal*, vol. 34, no. 6, 2021.
[75] P. Verma *et al.*, "Mrdace: An intelligent architecture for secure sharing and traceability of the medical images and patients' records," *ACM HEALTH*, vol. 6, no. 3, May 2025.
[76] M. Zichichi *et al.*, "Accountable clouds through blockchain," *IEEE Access*, vol. 11, pp. 48358–48374, 2023.
[77] Z. Liu *et al.*, "Data integrity audit scheme based on quad merkle tree and blockchain," *IEEE Access*, vol. 11, pp. 59263–59273, 2023.
[78] I. Mustafa *et al.*, "Smart contract life-cycle management: an engineering framework for the generation of robust and verifiable smart contracts," *Frontiers in Blockchain*, vol. 6, p. 1276233, 2024.
[79] T. Weingärtner *et al.*, "Prototyping a smart contract based public procurement to fight corruption," *Computers*, vol. 10, no. 7, 2021.
[80] S. Mohammed and D. Basheer, "Privacy preserving algorithm using chao-scattering of partial homomorphic encryption," *Journal of Physics: Conference Series*, vol. 1963, p. 012154, 07 2021.
[81] B. T. Hasan *et al.*, "Real-time resource monitoring framework in a heterogeneous kubernetes cluster," in *2022 Muthanna International Conference on Engineering Science and Technology (MICEST)*, 2022, pp. 184–189.
[82] U. Chohan, "Blockchain enhancing political accountability? sierra leone 2018 case," *SSRN Electronic Journal*, 01 2018.
[83] A. Canciani *et al.*, "Hybrid dlt as a data layer for real-time, data-intensive applications," 2023.
[84] A. Shahaab *et al.*, "A hybrid blockchain implementation to ensure data integrity and interoperability for public service organisations," in *IEEE International Conference on Blockchain*, 2021, pp. 295–305.
[85] O. Can *et al.*, "A blockchain-based hybrid architecture for auditable consent management," *IEEE Access*, vol. 12, pp. 100419–100445, 2024.
[86] G. Misiakoulis *et al.*, "Enhancing security and scalability in electronic voting through privacy-preserving cryptography and efficient data structures," in *2024 IEEE International Conference on Blockchain (Blockchain)*, 2024, pp. 631–636.
[87] B. Zhang *et al.*, "A blockchain and zero knowledge proof based data security transaction method in distributed computing," *Electronics*, vol. 13, p. 4260, 2024.
[88] X. Hu *et al.*, "Optimized cross-chain transactions with aggregated zero-knowledge proofs: Enhancing efficiency and security," *IEEE Internet of Things Journal*, vol. 12, no. 9, pp. 11495–11510, 2025.
[89] H. Eren *et al.*, "Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: A comprehensive review," *Applied Sciences*, vol. 15, no. 6, 2025.
[90] M. Xiao *et al.*, "Advanced security auditing methods for solidity-based smart contracts," *Electronics*, vol. 13, no. 20, 2024.
[91] N. Nousias *et al.*, "A process-aware approach for blockchain-based verification of academic qualifications," *Simulation Modelling Practice and Theory*, vol. 121, p. 102642, 2022.
[92] G. Ramakrishnan *et al.*, "Solidity vulnerability scanner," in *ICDSAAI*, vol. 01, 2022, pp. 1–5.
[93] C. Chambefort *et al.*, "Blockchain, tokens, smart contracts, and "decentralized autonomous organization": Expanding and renewing the mechanisms of governance," *EMR*, vol. 21, no. 3, pp. 511–515, 2024.
[94] D. Dhillon *et al.*, *Smart Contract Vulnerabilities: Exploring the Technical and Economic Aspects*. Springer Nature Switzerland, 2024, p. 81.
[95] F. Corradini *et al.*, "Engineering trustable and auditable choreography-based systems using blockchain," *ACM TMIS*, vol. 13, no. 3, Feb. 2022.
[96] A. Stocco *et al.*, "Software verification challenges in the blockchain ecosystem," *STTT*, 2024.

[97] Z. Deng *et al.*, "Enhancing blockchain cross chain interoperability: A comprehensive survey," 2025. [Online]. Available: https://arxiv.org/abs/2505.04934
[98] W. Wei *et al.*, "Beaiv: Blockchain empowered accountable integrity verification scheme for cross-chain data," in *Web Information Systems and Applications*. Singapore: Springer Nature Singapore, 2023, pp. 488–500.
[99] K. Nikolaos *et al.*, "The current state of interoperability between blockchain networks," European Commission, Technical Report, Nov. 2023.
[100] S. Lazzaro *et al.*, "Achieving accountability and data integrity in message queuing telemetry transport using blockchain and interplanetary file system," *Future Internet*, vol. 16, no. 7, 2024.
[101] K. Makhijani *et al.*, "Accountable and distributed industrial control systems with autonomous contracts : OCN-DLT," in *26th ICIN*, 2023.
[102] J. Kalbantner *et al.*, "A dlt-based smart contract architecture for atomic and scalable trading," *arXiv: Cryptography and Security*, 2021.
[103] A. Miller *et al.*, "Smart contracts and opportunities for formal methods," in *ISoLA*. Springer, 2018, pp. 280–299.
[104] A. Gurjar *et al.*, "Smart contract vulnerabilities and detection methods: A survey," in *15th ICCCNT*, 2024, pp. 1–7.
[105] S. M. Nzuva, "Revisiting blockchain technologies and smart contracts security: A pragmatic exploration of vulnerabilities, threats, and challenges," *Asian J. Res. Comput. Sci.*, vol. 17, no. 7, p. 11–30, Jun. 2024.
[106] C. Zeng *et al.*, "Smart contract vulnerability detection under digital assets," in *2024 4th CCSB*, 2024, pp. 515–519.
[107] H. Zhu *et al.*, "A survey on security analysis methods of smart contracts," *IEEE TSC*, vol. 17, no. 6, pp. 4522–4539, 2024.
[108] U. U. Ibekwe *et al.*, "Navigating the smart contract threat landscape: A systematic review," *IJEECS*, vol. 37, no. 2, pp. 1209–1224, 2025.
[109] P. Preethi *et al.*, "Smart contracts vulnerabilities detection using ensemble architecture of graphical attention model distillation and inference network," *IAES IJ-AI*, vol. 14, no. 1, 2025.
[110] J. Cheng *et al.*, "A vulnerability detection framework with enhanced graph feature learning," *ACM JSSO*, vol. 216, p. 112118, 2024.
[111] J. Huang *et al.*, "Smart contract vulnerability detection model based on multi-task learning," *Sensors*, vol. 22, no. 5, 2022.
[112] A. Makhijani *et al.*, "An extended access control model for permissioned blockchain frameworks," *Wireless Networks*, vol. 25, no. 8, 2019.
[113] D. Marbouh *et al.*, "Blockchain for covid-19: Review, opportunities, and a trusted tracking system," *AJSE*, vol. 45, 10 2020.
[114] G. Caldarelli, "Can artificial intelligence solve the blockchain oracle problem? unpacking the challenges and possibilities," 07 2025.
[115] S. Eskandari *et al.*, "Sok: oracles from the ground truth to market manipulation," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, ser. AFT '21. Association for Computing Machinery, 2021, p. 127–141.
[116] Karaduman *et al.*, "Blockchain-enabled supply chain management: A review of security, traceability, and data integrity amid the evolving systemic demand," *Applied Sciences*, vol. 15, no. 9, 2025.
[117] B. Chen et al., "A comprehensive survey of blockchain scalability: Shaping inner-chain and inter-chain perspectives," 2024. [Online]. Available: https://arxiv.org/abs/2409.02968
[118] M. Al-Zubaidie and W. Jebbar, "Blockchain-powered dynamic segmentation in personal health record," Mesopotamian Journal of Cybersecurity, vol. 5, pp. 2958–6542, 09 2025.