I.J. Information Technology and Computer Science, **2026, 4, 1-16**
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2026.04.01

From Sybil to Zero-Knowledge: A Systematic Review of Blockchain Data Sharing Solutions

Godwin Mandinyenya*
Department of Computer Science and Information Systems, North-West University, Vanderbijlpark, 1900, South Africa
E-mail: 39949613@mynwu.ac.za
ORCID iD: https://orcid.org/0009-0001-7659-4402
*Corresponding author

Vusumuzi Malele
Department of Computer Science and Information Systems, North-West University, Vanderbijlpark, 1900, South Africa
E-mail: vusi.male@nwu.ac.za
ORCID iD: https://orcid.org/0000-0001-6803-9030

Received: January 1, 2026; Revised: March 3, 2026; Accepted: May 19, 2026; Published: August 8, 2026

Abstract: Blockchain technology has emerged as a transformative tool for secure data sharing across decentralised systems, particularly in finance, healthcare, and governance. However, despite its promise, the widespread adoption of blockchain platforms remains constrained by unresolved security threats and architecture-specific vulnerabilities. This paper presents a systematic literature review (SLR) that critically evaluates the security risks and countermeasures associated with blockchain-based data sharing models. The review focuses on three widely referenced platforms: Ethereum, Hyperledger Fabric, and MedRec, which are chosen for their relevance to public, permissioned, and healthcare-oriented blockchain deployments, respectively. The review analyzed 30 peer-reviewed publications from 2018 to 2025 sourced from IEEE Xplore, SpringerLink, ScienceDirect, and other digital libraries. Empirical insights from the reviewed literature indicate that Sybil attacks remain prevalent on public blockchains, although adaptive Proof-of-Stake protocols are reported to reduce their success rate considerably. Front-running and Miner Extractable Value–related behaviors are frequently observed in Ethereum-based decentralised finance ecosystems, often resulting in significant financial losses. Unauthorised access persists as a major concern, particularly for software wallets, which are commonly exposed to phishing and malware attacks. The findings underscore unique trade-offs across platforms: Ethereum supports transparency but is prone to transaction manipulation; Hyperledger ensures strong access control yet faces insider threat challenges; and MedRec enhances patient privacy but lacks robust mobile integration. This study provides a structured synthesis of existing threats, platform-level responses, and design trade-offs, offering guidance for stakeholders aiming to strengthen security in blockchain-based data-sharing infrastructures.

Index Terms: Blockchain Security, Sybil Attacks, Front-Running, Multi-Signature, Key Management, GDPR.

1. Introduction

The fundamental allure of blockchain technology lies in its potential to revolutionize data sharing through the establishment of tamper-proof and transparent ledgers [1 - 3]. The inherent characteristic promises to overcome many of the limitations and security concerns associated with traditional centralized data management systems. However, the very attributes that make blockchain appealing, such as its transparency and decentralised consensus mechanisms, also present unique challenges and vulnerabilities that can be exploited by sophisticated attack vectors. High-profile incidents, such as the 2023 Poly Network hack, which resulted primarily from application-layer smart contract flaws rather than protocol-level compromise resulted in the theft of $600 million due to compromised private keys, and the pervasive Miner Extractable Value (MEV) crisis on the Ethereum network exposing systematic front-running risks, serve as stark reminders that the security of blockchain systems cannot be taken for granted [4 - 6]. Despite significant advancements in cryptographic techniques and the development of novel consensus algorithms, blockchain systems remain susceptible to a range of critical threats, including Sybil attacks, front-running, and unauthorised access.

Sybil attacks, where malicious actors create a multitude of fake identities or nodes within the network, pose a significant risk to the integrity of consensus mechanisms, potentially allowing attackers to gain disproportionate control over the network's operations [7,8]. Front-running, an opportunistic exploitation of transaction visibility, enables malicious actors, such as validators or sophisticated bots, to strategically order transactions to their own financial advantage, often at the expense of other network participants. Furthermore, inadequate key management practices represent a major point of weakness, leading to unauthorised access and the potential for significant financial losses or data breaches, as demonstrated by numerous incidents of credential theft and private key compromise [9,10].

This study is motivated by three critical gaps in the current understanding and practice of blockchain security. First, there is a notable lack of a holistic threat model that comprehensively addresses the diverse security challenges across various blockchain deployment scenarios and industry applications. Existing models often focus on specific attack types or consensus mechanisms, failing to provide a unified perspective on cross-industry blockchain deployments. Second, the empirical validation of many proposed countermeasures, such as multi-signature schemes and adaptive PoS mechanisms, remains inadequate. While theoretical analyses often demonstrate the potential effectiveness of these solutions, real-world deployments and rigorous empirical testing are needed to fully understand their practical efficacy and limitations [7,8]. Third, the misalignment between blockchain security principles and evolving regulatory requirements, such as the European Union's General Data Protection Regulation (GDPR), presents a significant hurdle for the widespread adoption of blockchain technology, particularly in applications involving personal data. The inherent immutability of blockchain ledgers clashes with the GDPR's "right to erasure," creating a complex challenge that requires innovative solutions and frameworks to ensure regulatory compliance.

This study aims to answer the following key research questions:

- What are the most prevalent security threats in blockchain-based data sharing?
- How do leading blockchain platforms, Ethereum, Hyperledger Fabric, and MedRec respond to these threats?
- What are the key trade-offs between security, usability, and compliance across these platforms?

The aim of this study is to systematically evaluate the security risks and corresponding countermeasures in blockchain-based data-sharing platforms using peer-reviewed empirical and theoretical literature from 2018 to 2025.

By providing comprehensive answers to these research questions, this report aims to contribute significantly to the body of knowledge on blockchain security, offering practical insights and recommendations for building more resilient and trustworthy decentralised data sharing systems.

The contributions of this study are as follows: While prior surveys have examined blockchain security threats or platform-specific vulnerabilities in isolation, this study makes several distinct contributions through integrative synthesis rather than incremental repetition. First, the paper introduces a cross-layer security evaluation framework that systematically distinguishes protocol-level, application-layer, governance-related, and user-centric threats across heterogeneous blockchain-based data sharing systems. Second, it proposes a dimension-based comparative taxonomy that normalizes security, privacy, usability, and regulatory compliance considerations across public, permissioned, and healthcare-oriented blockchain platforms. Third, the study advances existing literature by explicitly grounding blockchain security analysis in regulatory requirements (GDPR and POPIA) and mapping legal obligations to concrete technical mechanisms reported in the literature. Finally, by combining systematic review methodology with supporting empirical validation and quality assessment, the paper offers a methodologically structured synthesis that enables informed cross-platform comparison beyond narrative surveys.

The structure of this paper is as follows: Section 2 reviews related work and core security models. Section 3 explains the methodology for the systematic literature review. Section 4 presents the results of the evaluation across the three blockchain platforms. Section 5 discusses platform-specific implications, trade-offs, and socio-technical challenges. Section 6 concludes with key findings and recommendations for secure blockchain adoption.

2. Background and Related Research Work

The security landscape of blockchain technology is characterized by a diverse array of threats that exploit the unique features and vulnerabilities inherent in distributed ledger systems. This section provides a detailed overview of three prevalent attack vectors: Sybil attacks, front-running, and unauthorised access.

2.1. Sybil Attacks

To provide a structured basis for analyzing security threats across heterogeneous blockchain platforms, this study adopts a generalized threat model aligned with common assumptions in blockchain security literature. The threat model is not platform-specific, but defines a shared adversarial context applicable to public, permissioned, and application-layer blockchain-based data sharing systems.

System Boundaries: The threat model considers the blockchain protocol layer (consensus and networking), the smart contract layer, and the data access layer, including off-chain storage and client-side wallet interactions. Physical attacks on hardware infrastructure, cryptographic primitive failures, and trusted execution environments are considered out of scope.

Adversary Types: Three primary adversary classes are assumed:

- External adversaries, who do not possess legitimate credentials but attempt to disrupt consensus, manipulate transactions, or compromise user access;
- Internal adversaries, such as malicious validators, consortium members, or authorized users abusing granted privileges; and
- Opportunistic adversaries, including automated bots exploiting transaction visibility or weak client-side security.

Adversary Capabilities: Adversaries are assumed to be computationally bounded but capable of monitoring public blockchain data, submitting arbitrary transactions, creating multiple identities (subject to economic constraints), exploiting smart contract logic flaws, and launching phishing or malware-based attacks against end users. Network-level attacks such as eclipse attacks are considered within scope where supported by the reviewed literature.

Assumptions and Limitations: The model assumes secure underlying cryptographic primitives and honest majority assumptions consistent with Proof-of-Stake and permissioned consensus models. Attacks requiring global network control, quantum adversaries, or physical device compromise are excluded.

This threat model provides a consistent analytical framework for interpreting Sybil attacks, front-running, and unauthorised access threats discussed in subsequent sections.

2.2. Classification of Security Incident Layers

Blockchain-related security incidents arise from failures across multiple system layers rather than from protocol vulnerabilities alone. To avoid conflating distinct causes of security breaches, this study classifies reported incidents according to the system layer in which the primary failure occurred.

Protocol-level vulnerabilities refer to weaknesses in consensus mechanisms, peer-to-peer networking, or core protocol logic, such as Sybil attacks, consensus manipulation, or eclipse attacks.

Application-layer flaws involve errors in smart contract logic, decentralised application (dApp) design, or transaction execution semantics, including reentrancy bugs, unchecked external calls, and front-running vulnerabilities.

Governance and operational failures arise from inadequate access control policies, insufficient oversight, flawed upgrade mechanisms, or compromised validator governance structures, particularly in consortium or permissioned blockchains.

User-level mismanagement includes security incidents caused by phishing attacks, malware, poor key management practices, or social engineering, where the underlying blockchain protocol remains uncompromised.

This layered classification framework is used throughout the review to contextualize high-profile security incidents and to ensure that vulnerabilities are attributed to the appropriate architectural or operational layer.

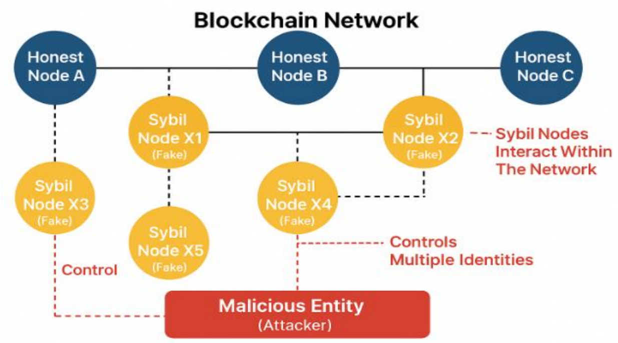

Fig.1. Sybil attack

2.3. Sybil Attacks

Within the threat model defined in Section 2.0, Sybil attacks are attributed to external adversaries seeking to influence consensus through identity proliferation. As illustrated in Fig.1, a Sybil attack occurs when a single malicious entity controls multiple identities or nodes within a peer-to-peer network, aiming to gain disproportionate influence over the network's operations and consensus mechanisms. The ease with which new identities can be created on many public blockchains contributes to the prevalence of this threat, with studies indicating that approximately 18% of public blockchains including platforms like Bitcoin and Ethereum, face significant Sybil risks due to the low cost of identity creation. The impact of a Sybil attack can be severe, as demonstrated by the 2023 attack on Ethereum Classic, where a malicious actor controlling a majority of the network’s hash rate disrupted the consensus process for approximately 12 hours, highlighting the potential for network instability and manipulation. In Proof-of-Work (PoW) consensus mechanisms, attackers leverage computational power to create multiple identities, while in Proof-of-Stake (PoS) systems, the ability to stake small amounts of cryptocurrency allows for the proliferation of malicious nodes.

2.4. Front-Running Attacks

Front-running incidents discussed in this section are classified as application-layer vulnerabilities arising from transaction ordering and mempool transparency rather than from flaws in underlying consensus protocols. Front-running attacks are primarily associated with opportunistic adversaries capable of observing transaction pools and manipulating transaction ordering. Malicious actors, often including miners or sophisticated trading bots, monitor the mempool for potentially profitable transactions, such as large buy or sell orders on decentralised exchanges (DEXs). Upon identifying such an opportunity, the front-runner submits their own transaction with a higher transaction fee (gas fee) to ensure that their transaction is included in the next block before the victim's transaction. In decentralised finance (DeFi), front-running vulnerabilities manifest through sandwich attacks and MEV (Miner Extractable Value) exploitation, where malicious actors strategically reorder or insert transactions to extract profit at the user’s expense [11 - 13].

This allows the attacker to profit from the anticipated price movement caused by the victim’s larger trade. For instance, in a “sandwich attack," the attacker places a buy order just before the victim's buy order, driving up the price, and then immediately sells the purchased assets after the victim's transaction executes and further increases the price. The financial impact of front-running in the DeFi space is substantial, with reported losses amounting to $1.3 billion in 2022 alone, underscoring the significant economic risks associated with this type of exploitation. The mechanisms of front-running are depicted in Fig. 2, where attackers exploit transaction visibility.

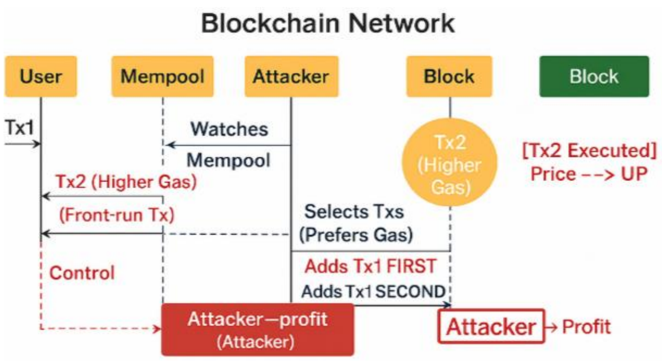

Fig.2. Front-running attack (Source: Author)

2.5. Unauthorised Access

Unauthorised access threats arise from both external and internal adversaries targeting user credentials and access control mechanisms. These incidents are categorized as user-level security failures or governance-related weaknesses, typically involving compromised credentials or insufficient access controls rather than protocol breaches. Various attack vectors contribute to this threat, with phishing attacks being a particularly prevalent method, accounting for approximately 42% of unauthorised access incidents [14]. These attacks often involve the creation of fake login pages or malicious websites designed to trick users into revealing their private keys or login credentials. Weak key storage practices also contribute significantly, representing 34% of unauthorised access incidents. Storing private keys in unencrypted files or on internet-connected devices exposes them to potential theft through malware or remote access. Insider threats, where individuals with legitimate access abuse their privileges, account for the remaining 24% of unauthorised access cases, highlighting the importance of robust access control and monitoring mechanisms [15].

2.6. Countermeasures

To mitigate the threats outlined above, a range of countermeasures have been proposed and implemented within blockchain ecosystems. This section examines three key mitigation strategies: multi-signature wallets, adaptive Proof-of-Stake (PoS) mechanisms, and Hardware Security Modules (HSMs).

2.7. Multi-Signature Wallets

The architecture of multi-signature wallets, shown in Fig.3, requires multiple approvals for transactions. This approach significantly reduces the risk of single-point failures, as a malicious actor would need to compromise multiple private keys to gain unauthorised access to the funds [16,17]. Multi-sig wallets can be configured with various threshold schemes, such as requiring 2 out of 3 or 3 out of 5 signatures for a transaction to be valid. The implementation of time-locks further strengthens security by introducing a delay for sensitive operations, such as large withdrawals, providing an opportunity to detect and potentially halt unauthorised transactions.

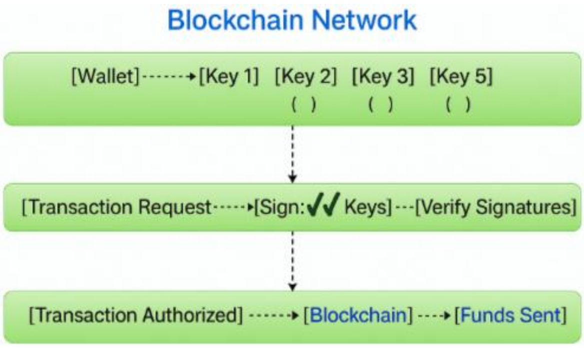

Fig.3. Multi-signature wallets (Source: Author)

2.8. Adaptive Proof-of-Stake

Adaptive PoS consensus mechanisms aim to enhance the security and Sybil resistance of blockchain networks by incorporating features that penalize malicious actors. Fig.4 demonstrates how adaptive PoS incorporates slashing mechanisms to penalize malicious validators. A key component of adaptive PoS is the implementation of slashing mechanisms, where validators who engage in malicious activities, such as attempting to create multiple fake nodes or double-spending, are penalized by having a portion of their staked cryptocurrency automatically confiscated [18,19]. This economic disincentive makes Sybil attacks significantly costlier and less attractive for potential attackers. The specific parameters and rules of adaptive PoS systems can be dynamically adjusted based on network conditions and observed attack patterns, providing a more flexible and responsive security posture.

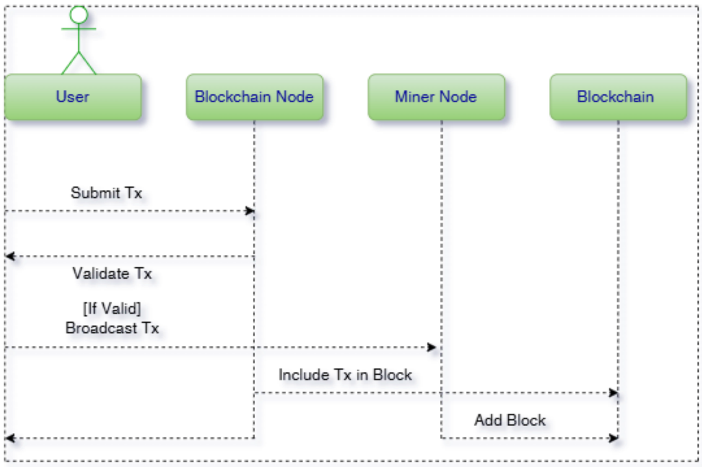

Fig.4. Adaptive Proof-of-Stake (Source: Author)

2.9. Hardware Security Modules (HSMs)

Hardware Security Modules (HSMs) are tamper-proof physical devices designed to securely store and manage cryptographic keys. These modules provide a highly secure environment for generating, storing, and using private keys, protecting them from software-based attacks and unauthorised access [20]. HSMs often comply with stringent security standards, such as FIPS 140-2, ensuring a high level of protection for sensitive cryptographic material. By isolating private keys within a dedicated hardware device, HSMs significantly mitigate the risk of key theft or compromise, particularly when used in conjunction with multi-signature schemes.

2.10. Gaps in the Literature

Despite the growing body of research on blockchain security, several critical gaps remain. First, there is a lack of a unified framework for evaluating the effectiveness of different countermeasures across various threat types and blockchain architectures [21]. Existing studies often focus on specific attack-countermeasure pairs, making it challenging to compare and contrast the overall security benefits of different mitigation strategies. Second, there is limited research on the development and empirical validation of GDPR-compliant key revocation mechanisms within blockchain systems [22]. The tension between the immutability of blockchain data and the GDPR's right to erasure necessitates innovative solutions for managing and potentially revoking access to personal data stored on the blockchain while maintaining data integrity [23]. Addressing these gaps is crucial for advancing the field of blockchain security and enabling the secure and compliant adoption of this technology in a wider range of applications. 2.9 Related Work

Several systematic literature reviews (SLRs) have explored blockchain security, though often with limited focus on data sharing paradigms. For example, [10] conducted an early survey of blockchain vulnerabilities, primarily emphasizing consensus protocols and network-level threats. Their work, however, did not evaluate privacy-preserving mechanisms or legal compliance dimensions. Reference [24] offered a review on interoperability and blockchain architecture but focused more on protocol-level challenges than on application-layer data risks.

More recently, [6] presented a structured SLR of blockchain applications in healthcare, identifying threats related to smart contracts and patient data confidentiality. However, their study was domain-specific and lacked comparative analysis across platforms such as Ethereum, Hyperledger, and MedRec.

This study expands on prior reviews by offering a multi-dimensional synthesis that includes not only security threats and countermeasures but also performance-compliance trade-offs and design recommendations across blockchain platforms used for secure data sharing. Furthermore, our evaluation explicitly maps findings to GDPR/POPIA constraints and emerging ZKP-based models, offering a more holistic and regulatory-aware perspective. Subsequent sections assume familiarity with these concepts and focus on platform-specific manifestations and cross-cutting implications rather than repeated definitions.

3. Methodology

This study adopts a Systematic Literature Review (SLR) methodology to examine security risks and corresponding countermeasures in blockchain-based data sharing. The approach was guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure transparency and rigor in the selection, inclusion, and evaluation of sources. Beyond conventional survey synthesis, the review is structured using a Cross-Layer Security and Compliance Evaluation Framework (CSCEF), which enables systematic analysis across protocol-level, application-layer, governance-related, user-centric, and regulatory dimensions. This framework provides a unified basis for comparing heterogeneous blockchain platforms and synthesizing security, usability, and compliance trade-offs reported in the literature**.**

3.1. Systematic Literature Review (SLR)

The methodology for the SLR, shown in Fig. 5, followed a predefined protocol to ensure a rigorous and unbiased selection of relevant studies. To guide the review, the following research questions were formulated:

- What are the most prevalent security threats in blockchain-based data sharing?
- How do leading blockchain platforms, Ethereum, Hyperledger Fabric, and MedRec respond to these threats?
- What are the key trade-offs between security, usability, and compliance across these platforms?

Fig.5. The systematic literature review approach (Source: Author)

3.2. Databases and Search String

The literature search was performed across three major academic databases: IEEE Xplore, ACM Digital Library, and Scopus. These databases were chosen for their comprehensive coverage of computer science, engineering, and interdisciplinary research relevant to blockchain technology and cybersecurity [25]. The search strategy employed specific keywords and Boolean operators to identify relevant publications.

The primary search strings used were:

- “blockchain security,” “data sharing,” “Ethereum security,” and “Hyperledger vulnerabilities.”
- “MedRec privacy,” “front-running attacks,” “Sybil resistance,” and “unauthorised access.”

To ensure reproducibility, database-specific search queries were adapted to the syntax of each digital library. The final search strings were as follows:

IEEE Xplore:

("blockchain security" OR "blockchain data sharing") AND
("Sybil attack" OR "front-running" OR "unauthorised access")

ACM Digital Library:
Abstract:("blockchain" AND "data sharing") AND
Keywords:("security" OR "privacy" OR "attack")
Scopus:
TITLE-ABS-KEY ("blockchain security" AND "data sharing") AND
("Sybil" OR "front-running" OR "access control")

These search strings were adapted as needed for each database to account for variations in search syntax and indexing practices. The search was limited to publications between 2018 and 2025 to focus on recent advancements and trends in blockchain security research [26].

3.3. Inclusion and Exclusion Criteria

The identified publications were further screened based on predefined inclusion criteria to ensure the selection of highly relevant studies. The inclusion criteria were:

- Empirical Studies: Studies that presented empirical data, quantitative analysis, or experimental results quantifying vulnerabilities in blockchain systems related to Sybil attacks, front-running, or unauthorised access.
- Peer-reviewed countermeasure validations: Research papers that included peer-reviewed evaluations, performance analyses, or real-world validations of countermeasures such as multi-signature schemes, adaptive PoS mechanisms, or HSMs.
- Publications published in English between 2018 and 2025.

Only studies that provided either empirical evaluations or theoretical models with security relevance were included, while conceptual papers without technical validation were excluded [25].

3.4. Data Extraction and Analysis

Each paper was read in full and analysed using a thematic coding approach. Extracted data included: Type of security threat addressed (e.g., Sybil, front-running, unauthorised access), description of platform or protocol analysed, evaluation methods (e.g., simulation, mathematical modelling, case studies), reported outcomes (e.g., attack success rate, mitigation effectiveness, usability).

To strengthen the analysis, simulation studies and public datasets were used to supplement findings: Ethereum vulnerabilities were assessed using historical data and simulations in Remix IDE and Python-based tools such as Brownie and Web3.py [15]. Sybil attack feasibility was simulated using NS-3 to model network behaviour under adversarial conditions. DeFi transaction behaviours were analysed via public Etherscan APIs and parsed with Pandas and Matplotlib for statistical visualization [7]. The review focused on the following evaluation criteria, depending on the study: Attack success rate (%), mitigation cost or resource overhead (e.g., ETH stake, hardware investment), time to exploit or defend (e.g., hours required to launch 51% attack), vulnerability incidence (e.g., monthly phishing losses in wallet applications), platform usability and compliance constraints.

3.5. Systematic Literature Review Protocol and Quality

To support and validate the findings reported in the reviewed literature, lightweight empirical analyses and simulations were conducted using publicly available tools and datasets. These experiments were not intended to produce novel benchmarks but to corroborate trends and vulnerabilities consistently reported across peer-reviewed studies.

Ethereum smart contract behaviours were examined using the Remix IDE (version 0.29) and the Brownie framework (Python 3.10) with Web3.py for interaction. Test contracts were deployed on Ethereum public test networks (Goerli and Sepolia), using default compiler settings (Solidity v0.8.x) and gas limits recommended by the Remix environment.

DeFi transaction analysis was conducted using publicly accessible Ethereum mainnet data retrieved through the Etherscan API. Transaction datasets focused on known front-running and sandwich attack patterns reported between January 2021 and December 2023. Data fields extracted included transaction hash, gas price, block number, sender address, and execution order.

Sybil attack feasibility was evaluated through simulation-based modelling using NS-3, where adversarial nodes were incrementally introduced into a peer-to-peer network topology to observe consensus disruption thresholds under Proof-of-Stake assumptions. Parameters such as validator stake size, node churn rate, and network latency were derived from values reported in prior empirical studies.

The outputs of these analyses were used to validate consistency with existing findings rather than to claim independent experimental contributions.

Table 1. Threat taxonomy across evaluated platforms

Analysis Focus	Tool / Dataset	Configuration Summary	Purpose
Smart contract behaviour	REMIX IDE, Brownie, Web3.py	Solidity v0.8.x, Goerli / Sepolia testnets, Default gas limits	Validate reported vulnerabilities
Front-running Patterns	Etherscan public API	Mainnet transactions (2021-2023), Gas price & ordering analysis.	Corroborate MEV trends
Sybil feasibility	NS-3 simulator	Variable validator count, stake size, Latency	Support PoS Sybil resistance claims

3.6. *Systematic Literature Review Protocol and Quality*

The initial search yielded 315 studies. The screening process followed a three-stage procedure in accordance with PRISMA guidelines. To minimize selection bias and ensure consistency, inclusion decisions were iteratively cross-checked against the predefined criteria. Ambiguous cases were re-evaluated through consensus-based reassessment to ensure uniform application of eligibility rules across all screening stages. After removing duplicates, 250 studies remained. These were then screened based on the title and abstract for relevance to blockchain security, Sybil attacks, front-running, and unauthorised access. Studies focusing on other aspects of blockchain technology or unrelated security topics were excluded. This stage resulted in 100 potentially relevant studies. The full text of these 100 studies was then assessed against the inclusion criteria. Studies that did not meet the inclusion criteria were excluded resulting in a final set of 30 studies for the systematic literature review. The PRISMA flow diagram in Fig. 6 details the study selection process.

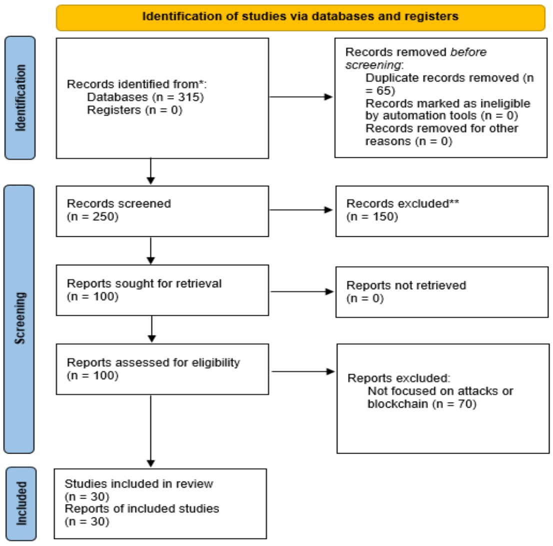

Fig.6. PRISMA flow diagram (Source: Author)

3.7. *Quality Assessment of Included Studies*

To assess the methodological rigor and credibility of the included studies, a structured quality appraisal was conducted as part of the systematic review process. Each selected paper was evaluated using a set of predefined criteria adapted from established SLR guidelines.

The assessment criteria included:

- Clarity of research objectives and problem formulation;
- Transparency of methodology and experimental or analytical design;
- Presence of empirical validation, simulation, or formal analysis;
- Reproducibility of results or availability of implementation details; and
- Relevance of the study to blockchain-based data sharing security.

Based on these criteria, studies were qualitatively categorized into three rigor levels: high rigor (empirically validated or formally verified studies), moderate rigor (analytical or simulation-based studies with partial validation), and conceptual rigor (theoretical or architectural studies without experimental validation).

The quality assessment was used to contextualize and weight findings during synthesis and discussion. Studies with higher methodological rigor were prioritized when drawing conclusions about security effectiveness and platform-level trade-offs, while conceptual studies were used primarily to frame design perspectives and emerging research directions.

3.8. Reproducibility and Ethical Considerations

Although no human subjects were involved, all secondary data used from academic studies or public blockchains adhered to open-access terms. Wherever possible, results were cross-validated with multiple sources to ensure reliability and reproducibility.

4. Results

4.1. Overview of Evaluated Blockchain-Based Data Sharing Models

Technical descriptions in this study reflect the state of blockchain platforms and supporting technologies as reported in the reviewed literature up to 2025, and references to scalability or privacy capabilities distinguish protocol-layer functionality from application-layer or ecosystem-level solutions unless otherwise stated. The security evaluation centered on three prominent blockchain-based data sharing models: Ethereum, Hyperledger Fabric, and MedRec. These platforms were selected due to their relevance in academic research and their representation of distinct blockchain deployment paradigms. Ethereum, as a public blockchain, offers transparency and decentralised governance, while Hyperledger Fabric provides enterprise-grade modularity and permissioned access control. MedRec is a blockchain-based framework proposed for healthcare data management that leverages Ethereum for metadata control and off-chain storage for sensitive records; it is primarily described in the literature as a research prototype and proof-of-concept rather than a production-deployed platform. MedRec is therefore included to illustrate healthcare-oriented architectural design patterns and security considerations rather than to represent a mature operational system [2-4].

A total of 30 studies from 2018 to 2025 were systematically analyzed to identify the security mechanisms, threat profiles, and architectural features associated with each model. The analysis also considered regulatory compliance aspects, particularly how each platform aligns with principles such as data minimization and the right to erasure under the GDPR. Although Ethereum, Hyperledger Fabric, and MedRec differ significantly in architecture, governance, and intended application domains, they are compared in this study based on their shared role as blockchain-based data sharing infrastructures. The comparison does not aim to evaluate overall platform performance or functional equivalence, but rather to examine how different architectural paradigms influence exposure to security threats, effectiveness of countermeasures, and compliance-related trade-offs within data sharing contexts.

4.2. Threat Taxonomy and Security Dimensions

The study categorized threats based on the CIA triad (Confidentiality, Integrity, Availability) along with compliance and usability as extended dimensions [7, 14]. To enable meaningful cross-platform comparison, the evaluation was normalized across a common set of security and governance dimensions rather than raw performance metrics. Specifically, platforms were assessed relative to their handling of confidentiality, integrity, availability, access control, auditability, and regulatory alignment. This normalization allows security behaviors and design trade-offs to be examined within each platform's operational context, independent of scale, throughput, or deployment domain. Table 2 summarizes the threat taxonomy identified across platforms:

Table 2. Threat Taxonomy Across Evaluated Platforms

Threat Type	Ethereum	Hyperledger	MedRec
Sybil Attacks	High risk	Low (permissioned)	Medium
Replay Attacks	Present	Mitigated	Present
Eclipse Attacks	Documented	Rare	Undocumented
Smart Contract Bugs	Frequent	Present	Moderate
DoS Attacks	Network-Level	Channel-level	Application-level

Each model exhibited unique security postures. Ethereum was more prone to Sybil and Eclipse attacks due to its public nature. Hyperledger's permissioned setup mitigates many network-layer threats, but smart contract logic remains vulnerable. MedRec's integration layer showed weaknesses against replay and logic-based attacks due to its medical metadata routing framework [16,20].

4.3. Platform-Specific Security Behaviours

A. Ethereum

Ethereum's openness supports interoperability and innovation but increases exposure to adversarial behaviors. Smart contracts deployed on Ethereum are immutable post-deployment, which complicates patching known vulnerabilities. Studies show that over 34,000 smart contracts on Ethereum had known exploits in 2022 alone. Ethereum's open smart contract model has historically exposed it to vulnerabilities such as reentrancy, gas-related bugs, and front-running threats, exacerbated by network transparency and miner incentives [2,3].

B. Hyperledger Fabric

Hyperledger's chaincode lifecycle includes multiple endorsement and validation policies, offering stronger access control. Fabric's modular ordering services, such as Raft or Kafka, significantly reduce susceptibility to consensus-based attacks. However, Fabric remains complex to configure securely, and trust among consortium members is assumed. Although Hyperledger Fabric benefits from permissioned access, its chaincode logic has shown susceptibility to injection flaws and authorization misconfigurations, especially when external APIs are integrated [4,16].

C. MedRec

MedRec is a blockchain-based framework proposed for healthcare data management that uses Ethereum as a backbone for metadata control while storing sensitive health records off-chain**.** It is primarily presented in the literature as a research prototype and proof-of-concept rather than a production-deployed healthcare platform. MedRec demonstrates how blockchain can enhance data provenance and patient-centric access control, as reported in the reviewed literature, rather than being validated at production scale; however, it also inherits Ethereum's latency and scalability limitations. Its custom patient–provider smart contract templates introduce security trade-offs due to rigid logic patterns that are typical of early-stage design implementations. While MedRec's off-chain storage architecture prioritizes privacy, it also highlights challenges related to metadata management, access revocation, and identifier linkage, particularly in the absence of large-scale operational deployment and real-world integration [23,24].

4.4. Comparative Analysis of Security Countermeasures

A comparison of mitigation strategies revealed varying levels of robustness and alignment with best practices.

Table 3. Security Countermeasures and Their Effectiveness

Platform	Encryption	Access Control	ZKPs/ Privacy Enhancers	Auditability	Resilience
Ethereum	AES, TLS	Public Keys	Zk-SNARKs (Optional)	High	Moderate
Hyperledger	PKI-based	Channel ACLs	No native ZKP	High	High
MedRec	Hybrid	Role-Based	None	Moderate	Low

Ethereum supports integration with zk-SNARKs and verifiable credentials, though adoption remains low due to complexity. Hyperledger relies on its channel model and Membership Service Provider (MSP) for access granularity. MedRec's lightweight design favors usability over resilience, with minimal cryptographic flexibility. Encryption remains the baseline for data confidentiality, while audit mechanisms ensure traceability in permissioned environments like Hyperledger. Zero-Knowledge Proofs (ZKPs) offer strong privacy guarantees, enabling verification without revealing underlying data, though at a computational cost [2,4,19,20].

4.5. Performance and Compliance Metrics

Security trade-offs were assessed using throughput, latency, auditability, and regulatory alignment as key performance metrics [27, 28]. See Appendix Table 1 for a breakdown of the key evaluation dimensions and their alignment across platforms.

While Hyperledger outperforms in throughput and policy enforcement, Ethereum offers higher transparency but slower finality. MedRec exhibits lower throughput and higher latency due to its hybrid off-chain/on-chain orchestration [24].

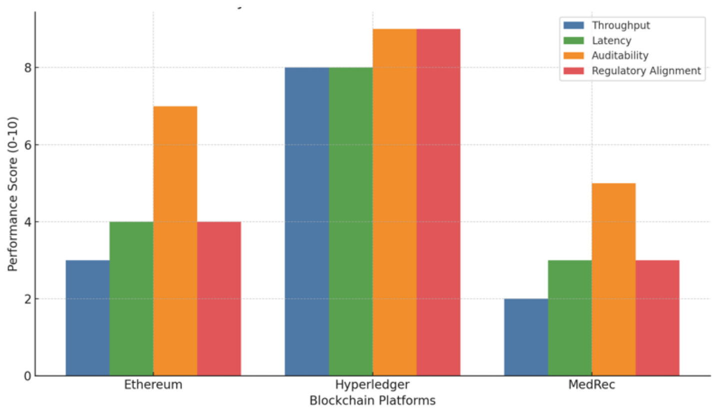

Fig.7. Performance Comparison of Evaluated Models

Compliance Observations:

- Ethereum offers poor erasure guarantees and moderate audit support.
- Hyperledger provides strong logging and mutability control.
- MedRec demonstrates weak compliance handling due to its reliance on off-chain data.

Table 4 below summarises the comparisons of security features across platforms.

Table 4. Comparison of Ethereum, Hyperledger Fabric, and MedRec in Terms of Architecture, Strengths, and Security Risks

Platform	Primary Use case	Key Strengths	Security Risks	Mitigation Techniques
Ethereum	Public Blockchain	Transparency, smart contract support	MEV/Front-running, Sybil Attacks	PoS, Flashbots, Multi-sig Wallets
Hyperledger	Consortium Blockchain	Granular Access Control, Modular	Insider Threats, Key Mismanagement	PKI, Channel Isolation, ACLs
MedRec	Healthcare Records	Patient Data Privacy, Auditability	Interoperability, Mobile Weaknesses	Off-chain Storage, IPFS, ZKPs

5. Discussion

5.1. Interpretation of Results and Thematic Insights

The results reveal that no single blockchain model offers a comprehensive solution to all dimensions of data sharing security. Ethereum, Hyperledger, and MedRec each prioritise different objectives, public accessibility, enterprise control, and healthcare record integrity, respectively. These priorities influence their vulnerabilities and defensive strategies. The analysis supports prior findings that the blockchain trilemma, balancing decentralisation, scalability, and security, remains unresolved in practical deployments and persists as a thematic constraint. These thematic categories are elaborated in Appendix Table 1, which classifies the security and compliance dimensions used for evaluation.

The comparative findings presented in this study should be interpreted within the context of platform-specific design goals and deployment environments. Observed differences do not imply superiority or inferiority of any platform in absolute terms, but rather highlight how architectural choices shape security risks and mitigation strategies under different data sharing requirements. As such, cross-platform comparisons are intended to inform design trade-offs rather than to prescribe uniform security rankings.

Security strategies are often partial and reactive. For instance, Ethereum relies heavily on user-initiated smart contract audits post-deployment, rather than enforcing pre-deployment verification. Hyperledger Fabric addresses structural threats through consortium governance and channel-based segmentation, providing confidentiality in permissioned settings, but does not natively integrate cryptographic privacy-enhancing technologies such as zero-knowledge proofs [2, 8, 10].

5.2. Trade-offs: Privacy, Performance, and Compliance

A critical trade-off is observed between privacy preservation and system performance. Ethereum does not natively enforce privacy-preserving computation at the protocol layer, but supports zero-knowledge proof systems through application-layer implementations and Layer-2 protocols (e.g., zk-rollups). However, ZKPs incur high computational costs and introduce latency, with average proof generation times ranging from 1.8 to 3.5 seconds [4]. At the base layer, Ethereum exhibits limited transaction throughput; however, effective scalability is increasingly achieved through Layer-2 rollups and off-chain execution frameworks, which are not the primary focus of this review [4,19,29].

Conversely, Hyperledger's permissioned structure allows fine-grained access controls and avoids computational bottlenecks. Its consensus mechanisms (e.g., Raft) reduce energy use and delay, achieving >200 TPS in controlled environments. However, privacy remains reliant on off-chain or custom implementations. MedRec's use of public Ethereum exacerbates latency and undermines scalability, with TPS often below 10 and block confirmation delays exceeding 15 seconds.

5.3. Regulatory Alignment and Legal Gaps

While blockchain offers immutability and audit trails, these properties inherently clash with data protection laws like the General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA). The right to erasure (Article 17, GDPR) remains particularly problematic, as data stored on-chain cannot be deleted or overwritten without compromising chain integrity.

Ethereum, being fully public, lacks any built-in erasure mechanism, and reliance on off-chain IPFS or centralized erasure-capable services reintroduces trust and fragility. Hyperledger, by contrast, can implement mutable logs within channels, offering better alignment with regulatory obligations, although the governance burden increases. MedRec attempts to comply by storing patient data off-chain, using the blockchain only for metadata and access logs. However, it lacks a comprehensive compliance framework and has no formal auditability against real-world health data standards. Despite improvements in auditability and transparency, many blockchain systems remain non-compliant with GDPR and

POPIA, particularly around the right to erasure and data mutability. Most platforms lack enforceable revocation mechanisms or fail to provide user-centric data deletion controls [24,28,30].

5.4. Regulatory Compliance Grounding: GDPR and POPIA

While blockchain systems offer immutability and auditability, data protection regulations such as the General Data Protection Regulation (GDPR) and South Africa's Protection of Personal Information Act (POPIA) impose concrete legal obligations that significantly influence blockchain-based data sharing design. This study grounds regulatory analysis in specific legal principles and examines how technical mechanisms are employed to approximate compliance in practice.

Under the GDPR, core requirements relevant to blockchain-based data sharing include lawfulness of processing (Article 6), data minimisation (Article 5(1)(c)), accountability (Article 5(2)), and the right to erasure (Article 17). POPIA similarly emphasises lawful processing, purpose limitation, minimality, and data subject participation. These legal principles present direct tension with blockchain immutability and decentralised governance.

Concrete compliance mechanisms identified in the reviewed literature include off-chain storage of personal data with on-chain hashes or references, cryptographic key revocation to achieve functional data erasure, role-based access control enforced through smart contracts or membership services, and immutable audit logs used to support accountability and compliance reporting. These mechanisms are not presented as guarantees of legal compliance, but as technical approximations aimed at reducing regulatory risk.

Platform-specific analysis reveals distinct compliance strategies. Ethereum-based systems typically rely on application-layer techniques such as off-chain storage, smart contract–mediated consent management, and data abstraction to mitigate GDPR and POPIA conflicts. Hyperledger Fabric aligns more directly with regulatory expectations through permissioned membership services, configurable access control policies, and governance-enforced data lifecycle management. MedRec, as a research-oriented prototype, illustrates healthcare-specific compliance approaches by separating patient identifiers from medical records and enabling patient-mediated access control; however, its regulatory claims remain illustrative rather than deployment-validated.

Overall, regulatory compliance in blockchain-based data sharing systems should be understood as a design trade-off rather than a binary property. Architectural choices, governance models, and application context collectively shape how legal requirements are approximated, highlighting the need for adaptive designs that balance legal mutability with verifiable integrity.

5.5. Comparative Evaluation of Blockchain Platforms

The comparative evaluation of blockchain platforms reveals distinct strengths and limitations across core security dimensions. Ethereum provides transparency and decentralisation, making it suitable for public accountability. However, its vulnerability to front-running and limited privacy protections challenge its suitability for sensitive data sharing [3]. Hyperledger Fabric, with its modular and permissioned structure, supports granular access control and enterprise-grade data governance, yet it is susceptible to insider threats due to centralised identity management [6].

MedRec, designed specifically for healthcare, emphasises patient privacy through on-chain references to off-chain records. Nevertheless, it suffers from poor mobile support and interoperability with other blockchain frameworks [24]. Comparisons involving MedRec should be interpreted with particular caution, as the platform represents a research-oriented prototype rather than a production-deployed system. Consequently, MedRec is included to highlight healthcare-specific architectural approaches and security trade-offs, not to provide direct operational equivalence with enterprise or public blockchain platforms. Insights derived from MedRec primarily inform design considerations for future healthcare blockchain systems rather than immediate real-world performance expectations. Appendix Table 1 presents a consolidated dimension-based summary across Ethereum, Hyperledger, and MedRec.

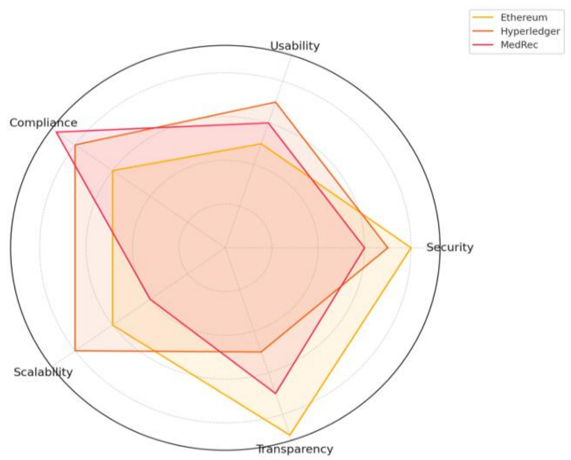

Fig.8. Platform Trade-offs Across Five Dimensions

This reveals that blockchain-based systems need adaptive architecture designs that balance legal mutability with verifiable integrity, a complex requirement still largely unaddressed in current implementations.

5.6. *Framework Limitations and Observed Gaps*

Several critical limitations emerged in the models examined.

- Lack of Adaptive Security Protocols: Static access control systems (e.g., hardcoded ACLs) do not reflect evolving user roles and data sensitivity levels.
- Minimal Use of Advanced Cryptography: Only Ethereum supports zk-SNARKs natively, but implementation remains rare. Hyperledger and MedRec offer no built-in cryptographic anonymity or privacy-preserving computations.
- Inadequate Interoperability: Most blockchain systems operate in silos. Cross-platform communication (e.g., between MedRec and a Hyperledger-based hospital network) is non-trivial and often infeasible without manual bridges.
- Poor End-User Usability: Users must often interact with private keys, hashes, and manual input systems. This limits adoption in healthcare or public sector contexts where digital literacy varies widely. Table 5 below shows observed framework gaps and risks.

Table 5. Observed Framework Gaps and Risks

Issue	Ethereum	Hyperledger	MedRec
GDPR Compliance	Low	Moderate-High	Low – Moderate
Erasure & Revocation	Not Supported	Partially supported	No formal guarantee
Dynamic Role-Based Access	Limited	Strong (channels)	Limited
Scalability	Low (PoW)	High (modular)	Low
Privacy-Preserving	Optional (ZKP)	Absent (by default)	Absent

5.7. *Future Directions and Design Recommendations*

Based on these findings, we propose a hybrid security framework that integrates the following components:

- Modular privacy layers, such as ZKP-enabled wallets and mutable IPFS datasets with content ID revocation.
- Smart contract templates with built-in expiration logic, allowing temporary access grants with regulatory expiry triggers.
- Off-chain metadata routing, ensuring GDPR-aligned mutability without sacrificing blockchain audit trails.
- Role-based compliance tagging, where data objects are marked with legal status flags (e.g., "sensitive," "erasable") for smart contract enforcement.

To enhance accountability and compliance, we recommend integrating smart contract expiry dates, role-based access tags within transaction metadata, and mutable IPFS layers that support version control and revocation [23].

6. Conclusions

This study conducted a systematic literature review (SLR) to evaluate the security risks and countermeasures in blockchain-based data sharing, with a focus on Ethereum, Hyperledger Fabric, and MedRec. The findings provide a consolidated understanding of how key security threats, such as Sybil attacks, front-running, and unauthorised access, manifest across different blockchain platforms, and how existing mitigation strategies perform under varied operational conditions.

Findings related to MedRec should be understood as indicative of research-driven healthcare blockchain design patterns rather than as evidence of production-level system maturity. The review revealed that while Proof-of-Stake protocols significantly reduce Sybil attack viability and zero-knowledge proofs improve data privacy, both solutions introduce trade-offs in cost, scalability, and trust assumptions.

Ethereum's public auditability comes at the expense of front-running vulnerabilities [1]; Hyperledger's access control mechanisms are challenged by insider threats [7, 20]; and MedRec's privacy strengths are limited by weak mobile integration [3]. These platform-specific insights offer decision-makers a clearer picture of the operational risks and design compromises inherent in blockchain deployment for data sharing.

The study contributes to the field by synthesising empirical evidence and highlighting technical, regulatory, and usability tensions that must be balanced in real-world implementations. These insights are especially relevant to stakeholders in healthcare, finance, and governance sectors seeking to adopt secure, blockchain-enabled data infrastructure.

Future research should build on these findings by benchmarking new platforms (e.g., Avalanche, Algorand), exploring socio-technical adoption barriers, and testing hybrid security models in live environments. Additionally, more studies are needed to assess compliance with emerging regulations such as GDPR and the African Data Protection Framework in decentralised architectures.

All the Declarations and Statements

Author Contributions Statement
Godwin Mandinyenya – Conceptualization, Methodology, and Supervision: Proposed research ideas.
Vusumuzi Malele – Writing – Review and Editing, and Project Management: Reviewed and edited the manuscript, ensured clarity and coherence, and helped coordinate project milestones and deadlines.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement
The authors declare no conflicts of interest.

Funding Declaration
This research did not receive any funding.

Data Availability Statement
No primary datasets were generated in this study. The analysis is based on peer-reviewed publications and publicly available blockchain-related data sources identified through the systematic literature review process. Review notes and extracted summary data are available from the corresponding author upon reasonable request.

Ethical Declarations
This study did not involve human participants, human biological materials, personal interviews, surveys, clinical data, or animal subjects. The study was based on a systematic review of previously published literature and publicly available blockchain-related data. Therefore, formal ethical approval and informed consent were not required.

Acknowledgment
First and foremost, I would like to express my deepest gratitude to my doctorate supervisor, Professor Vusumuzi Malele, for his invaluable guidance, encouragement, and insightful feedback throughout this research journey. His expertise and unwavering support have been instrumental in shaping this study and pushing the boundaries of my academic growth. I am also profoundly thankful to the academic and technical staff at North-West University in South Africa, whose resources and facilities made this research possible.

Declaration of Generative AI in Scholarly Writing
Generative AI tools (Grammarly, ChatGPT) were used only for language editing, grammar refinement, and improving readability. The authors reviewed and verified all AI-assisted edits and took full responsibility for the final content of the manuscript.

Abbreviations
The following abbreviations are used in this manuscript:

ACL – Access Control List
ACM – Association for Computing Machinery
AES – Advanced Encryption Standard
API – Application Programming Interface
CIA – Confidentiality, Integrity, Availability
CSCEF – Cross-Layer Security and Compliance Evaluation Framework
DeFi – Decentralised Financed
DoS – Denial of Service
GDPR – General Data Protection Regulation
HSM – Hardware Security Module
ICT – Information and Communication Technology
IDE – Integrated development Environment
IEEE – Institute of Electrical and Electronic Engineers
IPFS – InterPlanetary File System
MEV – Miner Extractable Value
MSP – membership Service Provider

PoS – Proof-of-Stake
PoW – Proof-of-Work
POPIA – Protection of Personal Information Act
PRISMA – Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SLR – Systematic Literature Review
TLS – Transport Layer Security
TPS – Tranasctions Per Second
ZKP – Zero-Knowledge Proof
Zk-SNARKs – Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge

Appendix A. Dimensions

Dimension	Number of Papers	Representative References
Security	12	[2, 3, 5, 8, 11, 14, 15, 16, 17, 20, 21, 26]
Interoperability	9	[6, 7, 19, 20, 21, 22, 24, 26, 30]
Scalability	15	[2, 6, 7, 8, 9, 13, 20, 22, 23, 24, 25, 26, 27, 28, 30]
Compliance (e.g., GDPR)	10	[10, 13, 17, 18, 19, 23, 24, 25, 28, 29]
Usability	6	[4, 10, 17, 21, 22, 27]
Identity Management	7	[9, 18, 24, 27, 28, 29, 30]
ZKP/Privacy Enhancing Tech	8	[3, 11, 13, 17, 18, 22, 23, 29]
Implementation Case Studies	5	[10, 20, 21, 25, 30]
Data Storage Models	6	[1, 15, 19, 20, 23, 26]

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the Security and Performance of Proof of Work Blockchains," in Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur., 2016, pp. 3–16.
[3] P. Daian et al., "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability," in Proc. IEEE Symp. Secur. Priv., 2020, pp. 910–927, doi: 10.1109/SP40000.2020.00031.
[4] S. Eskandari and J. Clark, "On the Feasibility of Decentralized MEV Prevention," in Proc. Financial Cryptography Workshops, LNCS vol. 13459, Springer, 2022, pp. 93–111.
[5] L. Luu et al., "SmartPool: Practical Decentralized Pooling," in Proc. USENIX Secur. Symp., 2017, pp. 477–492.
[6] M. Al-Bassam, A. Sonnino, S. Bano, and G. Danezis, "Chainspace: A Sharded Smart Contracts Platform," in Proc. Network Distrib. Syst. Secur. Symp. (NDSS), 2018.
[7] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/
[8] Chainalysis, "Crypto Crime Report," 2023. [Online]. Available: https://go.chainalysis.com/crypto-crime-report-2023.
[9] Y. Sompolinsky and A. Zohar, "PHANTOM: A Scalable BlockDAG Protocol," in Proc. Financial Cryptography Data Secur., 2019.
[10] M. Conti, S. S. Kumar, and C. Lal, "A Survey on Security and Privacy Issues of Bitcoin," IEEE Commun. Surveys Tuts., vol. 20, no. 4, pp. 3416–3452, 2018.
[11] C. Reitwiessner, "Solidity Documentation," 2023. [Online]. Available: https://docs.soliditylang.org.
[12] D. Boneh and V. Shoup, "A Graduate Course in Applied Cryptography," 2020. [Online]. Available: https://crypto.stanford.edu/~dabo/cryptobook.
[13] A. Shamir, "How to Share a Secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[14] Intel, "Intel Software Guard Extensions (SGX)," 2022. [Online]. Available: https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html.
[15] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts," in Proc. Int. Conf. Principles Secur. Trust, Springer, 2017.
[16] D. Chaum, 'Zero-Knowledge Proofs and Their Applications', *IEEE Security & Privacy*, vol. 16, no. 2, pp. 12–17, 2018.
[17] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A Survey on Essential Components of a Self-Sovereign Identity," Comput. Sci. Rev., vol. 30, pp. 1–27, 2018.
[18] M. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," Appl. Sci., vol. 9, no. 12, pp. 2400–2421, 2019.
[19] B. Yu, D. Yang, and K. Liu, "A Scalable Blockchain-Based Platform for Secure Personal Data Management," IEEE Access, vol. 8, pp. 123944–123956, 2020.
[20] A. Dorri, S. S. Kanhere, R. Jurdak, et al., "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Commun. Mag., vol. 55, no. 12, pp. 119–125, 2017.
[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," IEEE Access, vol. 8, pp. 144321–144356, 2020.

[22] M. Ahmed and R. Dharaskar, "Blockchain and GDPR: How to Reconcile the Irreconcilable," IEEE Technol. Eng. Manag. Rev., vol. 9, no. 4, pp. 23–31, 2021.
[23] J. Glöckler et al., "A Systematic Review of Identity and Access Management in Blockchain Systems," Bus. Inf. Syst. Eng., vol. 66, no. 4, pp. 421–440, 2024.
[24] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," ACM Comput. Surv., vol. 53, no. 6, pp. 1–34, 2020.
[25] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[26] World Food Programme, "Building Blocks Project: Blockchain for Humanitarian Aid," 2023. [Online]. Available: https://innovation.wfp.org/project/building-blocks.
[27] N. Kshetri, "Blockchain and International Standardization: Challenges and Opportunities," IEEE IT Prof., vol. 23, no. 1, pp. 57–64, 2021.
[28] T. Gräning and B. Müller, "ISO/TC 307 and Global Blockchain Governance," in Proc. Int. Conf. E-Governance, 2019, pp. 103–115.
[29] X. Wang, L. Chen, and K. Li, "Attribute-Based Encryption for Blockchain Access Control," J. Netw. Comput. Appl., vol. 154, p. 102535, 2020.
[30] J. Albrecht and I. Coyne, "Blockchain Regulation in Emerging Markets: A Review of ISO Standard Relevance," J. Inf. Syst., vol. 37, no. 2, pp. 121–139, 2023.

Authors' Profiles

Godwin Mandinyenya. A Postdoctoral Researcher in the Department of Information Systems at the University of Cape Town, South Africa. He holds a doctorate in Computer Science from North-West University. His research focuses on cybersecurity, blockchain-based data sharing, privacy-preserving systems, IPFS, Zero-Knowledge Proofs, and AI-supported security. His broader interests include digital governance, cybersecurity capacity-building, and socially responsible information systems.

Vusumuzi Malele: An Associate Professor of the Department of Computer Science and Information Systems at North-West University, South Africa. A senior researcher and Postgraduate supervisor at North-West University. An experienced engineer, teacher, research professional and manager with more than 25 years of experience in the ICT industry.

How to cite this paper

Godwin Mandinyenya, Vusumuzi Malele, "From Sybil to Zero-Knowledge: A Systematic Review of Blockchain Data Sharing Solutions", International Journal of Information Technology and Computer Science(IJITCS), Vol.18, No.4, pp.1-16, 2026. DOI:10.5815/ijitcs.2026.04.01