Advances in Artificial Intelligence and Machine Learning; Review 5 (1) 3373-3388 Received 04-12-2024; Accepted 15-03-2025; Published 21-03-2025

A Comprehensive Review of Interoperability Challenges and Applications Beyond Cryptocurrencies

Abdulrahman A. Alzahrani AMOHAMMEDALZAHRANI0010@STU.KAU.EDU.SA
Department of Computer Science,
Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah City,
Saudi Arabia.

Amin Y. Noaman ANOAMAN@KAU.EDU.SA
Department of Computer Science,
Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah City,
Saudi Arabia.

Ahmed A A. Gad-Elrab AAAHMAD4@KAU.EDU.SA
Department of Computer Science,
Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah City,
Saudi Arabia.

Fathy E. Eassa FEASSA@KAU.EDU.SA
Department of Computer Science,
Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah City,
Saudi Arabia.

Maher Khemakhem MAKHEMAKHEM@KAU.EDU.SA
Department of Computer Science,
Faculty of Computing and Information Technology,
King Abdulaziz University,
Jeddah City, Saudi Arabia.

Faisal Albalwy FBALWY@TAIBAHU.EDU.SA
Department of Cybersecurity,
College of Computer Science and Engineering,
Taibah University, Madinah 42353,
Saudi Arabia.

Hosam Aljihani HJIHANI@TAIBAHU.EDU.SA
Department of Computer Science,
College of Computer Science and Engineering,
Taibah University, Madinah 42353,
Saudi Arabia.

Corresponding Author: Abdulrahman A. Alzahrani

Citation: Abdulrahman A. Alzahrani, et al. A Comprehensive Review of Interoperability Challenges and Applications Beyond Cryptocurrencies. Advances in Artificial Intelligence and Machine Learning. 2025;5(1):193.

Abstract

The present study aimed to establish and evaluate the interoperability mechanisms such as sidechains, hashed time-lock contracts (HTLCs), blockchain bridges, smart contracts, and relay chains related to cross-chain communication across various industries. Utilizing PRISMA guidelines, the review identifies key challenges, including the absence of standardized protocols, security vulnerabilities, and governance complexities in heterogeneous systems. Cryptographic techniques like Zero-Knowledge Proofs (ZKP), Hybrid Connectors, and Threshold Signatures demonstrate significant potential for enhancing privacy and secure data exchange. The finding highlights the transformative potential of blockchain interoperability beyond cryptocurrencies, particularly in sectors like healthcare, education, and supply chain management. The study underscores the importance of developing standardized frameworks and innovative solutions to foster seamless integrations across blockchain ecosystems, unlocking blockchain's full potential in diverse applications.

Keywords: Blockchain interoperability, Cross-Chain communications, Decentralized systems, Zero-Knowledge proofs, Healthcare applications.

1. INTRODUCTION

Blockchain Technology (BCT) has gained popularity, especially due to the success of Bitcoin, as an effective technology for revolutionizing business models, reducing risk, and enhancing data handling [1]. Blockchain technology was introduced in 2008 through Bitcoin, since then it has revolutionized data storage and decentralized application frameworks by ensuring immutability, transparency, and security. The evolution of blockchain has stretched beyond cryptocurrencies into sectors like supply chain management, healthcare, and the Internet of Things (IoT), remodeling the interaction of industries with digital ecosystems [2, 3]. With the rapid growth of data, managing this data has created challenges in terms of privacy, authenticity, and accessibility. The siloed nature of blockchain networks performing independently with their consensus algorithms, governance models, and cryptographic protocols has led to interoperability challenges. These isolated ecosystems, often referred to as "Value islands," obscure the seamless exchange of assets and data, hindering blockchain's potential for wide-range, cross-domain applications [4, 5]

Blockchain interoperability refers to the ability of different blockchain platforms to connect [6], allowing users to access data, execute transactions, and share information across multiple chains [7]. The NIST definition affirms that various heterogeneous or homogeneous blockchains can carry out atomic transactions where data recorded in one blockchain is ready for use, verifiable, and referable to another [8]. Interoperability among heterogeneous blockchains has become an integral focus in blockchain research and development. Contrary to homogenous systems, heterogeneous blockchains vary remarkably in architecture, consensus mechanisms, and functionality, complicating cross-chain communications [9]. Real-world implementation remains difficult. Various public, private, and hybrid blockchain categories offer different advantages and disadvantages depending on organizational needs, with Cosmos and Polkadot being prominent examples [10].

Closing the divide necessitates solutions that call upon issues of standardization, scalability, and security while ensuring trustless environments that eradicate dependence on centralized intermedi-

aries. Mechanisms such as Sidechains, hashed time lock contracts (HTLCs) and blockchain bridges attempt to mitigate these challenges but face hindrances in scalability, security, and efficiency when applied to diverse blockchain [11, 12] Relays, classified as either trustless [13] or trusted [14], verify blockchain transactions, while blockchain-agnostic protocols aim to build an abstraction layer for communication across various blockchains [15], blockchain bridges and cross-chain communication protocols, eliminate third-party reliance, facilitating seamless interactions between heterogeneous blockchain networks [16]. Smart contracts are instrumental in automating agreements and ensuring secure and efficient data exchanges [16, 17]. Blockchain and smart contracts have many potential uses outside of the financial sector, including in insurance claims processing, supply chain management, and IP enforcement. The use of smart contracts and blockchain applications among businesses shows no signs of slowing down [18]. With smart contracts, blockchain technology may go beyond conventional contracts by automatically carrying out the terms of agreements between two or more people in a decentralized setting once the necessary circumstances have been satisfied [19].

The gravity for interoperability is specifically important for surfacing applications in non-cryptocurrency domains. For example, in healthcare, secure interoperability among blockchains could allow the trade of sensitive patient data between providers, improving care delivery could facilitate the exchange of sensitive patient data between providers, enhancing care delivery [20]. Likewise, in the case of supply chain management, cross-chain communication may warrant real-time visibility across ledgers, improving efficiency and trust between stakeholders [21]. The agricultural sector improves the tracking of the quality of products to guarantee that consumers are provided with adequate information about the food they consume [22]. Blockchain opens novel possibilities for the storage of student learning records. The actual work that students have completed in a lab or a service-learning project, as well as the As and Bs along with the course titles, can be kept in the student's records using the blockchain's built-in smart contract mechanism. Employers can view jobseekers more thoroughly and so make better decisions [23] Latest advancements like relay chains in platforms such as Polkadot and Cosmos along with cryptographic innovations like zero-knowledge proofs and hybrid connectors, have exhibited the potential to prevail over these barriers. Nonetheless, gaps in standardization and robust trustless bridging mechanisms persist, warranting further exploration and innovation [24]. There is no standardized method for communication between blockchain systems and the Internet [25], nor is there a trustless binary bridge for exchanging data across heterogeneous blockchains [6, 26].

A convincing solution for addressing these challenges requires leveraging the combination of blockchain bridges and smart contracts. This approach ensures secure and automated data exchanges between heterogeneous systems as well as reduces reliance on third-party intermediaries, strengthening decentralization. Smart contracts utilized within blockchain bridges can drastically improve data integrity, privacy, and trustlessness, allowing efficient and secure interoperability among platforms. Contrary to notary-based solutions that reintroduce centralization, this technique allows the development of decentralization while offering flexibility in transferring diverse data types [27].

The present study explored critical gaps, pressing upon the need for standardized frameworks and scalable, secure solutions. Expanding blockchain's utility beyond cryptocurrencies aimed to provide a roadmap for innovation in diverse sectors, facilitating seamless integration of decentralized systems. It seeks to build a foundation for future research and development in blockchain interoperabil-

ity. The goal is to enable blockchain networks to operate as interconnected ecosystems, unlocking their full potential for cross-domain applications and fostering innovation across industries. With blockchain's transformative potential increasingly recognized, achieving interoperability is crucial for advancing its adoption and impact in the digital area.

2. LITERATURE REVIEW

Blockchain interoperability has emerged as a critical research focus within decentralized systems. Applications such as cryptocurrency transactions, healthcare data sharing, and supply chain management have underscored the need for effective cross-chain communication solutions. However, existing mechanisms continue to face challenges related to scalability, security, and governance.

Early blockchain implementations functioned as isolated networks, creating what researchers describe as 'Value Islands' (Wust&Gervais,2018). The concept of interoperability refers to the ability of different blockchains to seamlessly exchange data, conduct transactions, and interact without intermediaries [5]. The National Institute of Standards and Technology (NIST) defines interoperability as the ability of heterogenous or homogenous blockchains to execute atomic transactions while ensuring data accessibility and verification [8]. Another perspective, provided by Lombard-Platte and Lafourcade (2020), describes interoperability as the connection of multiple blockchain networks to facilitate asset transfers and smart contract execution.

Several interoperability mechanisms have been developed to address these challenges. Sidechains allow asset transfers between a primary blockchain and auxiliary blockchains through two-way pegs [28]. This method enhances scalability by offloading transactions while maintaining a connection to the main chain. For instance, Bitcoins' Liquid Network employs sidechains to improve transactional privacy and reduce confirmation times [29]. However, reliance on third-party entities raises concerns about decentralization.

Hashed Time-Lock Contracts (HTLCs) facilitate atomic swaps by using cryptographic locks, ensuring simultaneous execution of transactions across blockchains [30]. While HTLC eliminates intermediaries, they require participating blockchains to support compatible cryptographic primitives, limiting their applicability in heterogeneous environments.

Blockchain bridges have also gained prominence as a mechanism for enabling interoperability. These bridges serve as connectors between different blockchains, allowing for asset transfers and data exchange. Notable examples include the Wormhole and Polygon bridges, which facilitate communication between Ethereum, Solana, and other networks [31]. Despite their advantages, blockchain bridges remain susceptible to security vulnerabilities, as demonstrated by the $320 million Wormhole exploit in 2022 [32].

Relay chains, pioneered by Polkadot and Cosmos, provide another approach to interoperability. Polkadot's relay chain enables secure asset and message exchanges between connected parachains, while Cosmo's Inter-Blockchain Communication (IBC) protocol allows modular and scalable interactions between diverse blockchain ecosystems [16, 24]. However, these solutions still face challenges in integrating blockchains with unique architectures [33].

Smart contracts, especially in private blockchains, could address major key challenges in identity management, consensus protocols, and cryptographic techniques. The lack of research on this integration warrants further studies on the application of smart contracts across various industries. An amalgamation of smart contracts with blockchain bridges provides ease of access in data exchanges, relieving third-party intermediation and privacy support moving toward new possibilities for cross-chain interoperability [27].

Advancements in cryptographic techniques have introduced promising interoperability solutions. Zero-knowledge proofs (ZKPs) enable privacy-preserving cross-chain interactions by verifying transactions without exposing sensitive information [34]. A study conducted in 2023 proposed a novel ZKP-based protocol for healthcare applications, demonstrating enhanced scalability and privacy protection [35]. Similarly, threshold signatures have been explored as a method for securing blockchain bridges by distributing private key management among multiple parties [36].

Hybrid connectors are another innovative approach, enabling secure communication between public and private blockchains. These connectors allow permissioned and permissionless blockchains to interact while maintaining security and privacy standards [37]. A notable example is the use of hybrid connectors in supply chain management, where Hyperledger Fabric and Ethereum were integrated to ensure end-to-end transparency [38]

Decentralized identity (DID) solutions, like those built on World Wide Web Consortium (WC3) standards, have been explored into blockchain interoperability frameworks. For example, a study in 2023 displayed the use of DID systems to improve cross-chain authentication along with user privacy in financial applications [38] These improvements correlate with the increasing pressure of user-centric interoperability frameworks.

The absence of standardization protocols for cross-chain communication remains a strong barrier. The lack of a unified framework for interoperability solutions catered to specific blockchains must be addressed to increase complexity and decrease scalability [39]. The vulnerability of interoperability mechanisms to frequent attacks like replay attacks or double-spending. Cross-chain bridges in particular recurring targets of exploits because of their complexity and dependency on smart contracts [40]. Another crucial challenge to maintain security and decentralization is scalability. A lot of the solution lacks and are unable to handle high-volume transactions, restricting their applicability to real-world use cases [41]. Disparities in governance structures between blockchains meddle with interoperability. In the case of permissioned blockchains, strict access controls are required. However, public blockchains allow open participation. Ensuring compatibility among diverse systems warrants the development of adaptive governance frameworks [21].

3. METHODOLOGY

3.1 Study Design and Search Strategy

This review utilizes a qualitative amalgamation of existing literature. Databases such as *Scopus, IEEE, Science Direct, Springer, ACM, and MDPI* were used to retrieve relevant literature. The Keywords *"blockchain interoperability, consensus mechanisms, standardization protocols,* blockchain interoperability *scalability* and *security, decentralization,* interoperability solutions in *healthcare*,

interoperability solutions in *education, and* interoperability solutions in *supply-chain"* were used to find studies. The search parameters were limited to English peer-reviewed articles published from 2015 to 2024 for the relevancy of the data.

3.2 Inclusion Criteria

A total of 17,559 studies were initially identified from selected databases. The filtering process began with keyword-based filtering, which reduced the number of studies to 9.048 by selecting articles relevant to blockchain interoperability. This was followed by title-based filtering, which further narrowed the selection to 5,450 studies by excluding papers unrelated to blockchain interoperability, consensus mechanisms, or cross-chain communication. The abstract screening was then conducted, retaining 3000 studies that contained sufficient information on interoperability challenges and solutions. Full-text screening was applied to assess the relevance of the remaining studies, resulting in 1,140 studies for further evaluation. A detailed full-text review ensured methodological rigor and substantive insights, reducing the count to 283 studies. Cross-validation was performed by comparing extracted studies against authoritative blockchain publications, and peer review was conducted by experts, maintaining the 283 studies. Finally, 37 studies were selected based on their methodological robustness, relevance to interoperability mechanisms, and contribution to addressing interoperability challenges beyond cryptocurrency.

The inclusion criteria encompassed studies that identified blockchain interoperability issues and solutions, evaluated their effectiveness, and explored applications in various sectors beyond cryptocurrencies. This approach facilitated comparative analysis and the identification of research gaps.

3.3 Exclusion Criteria

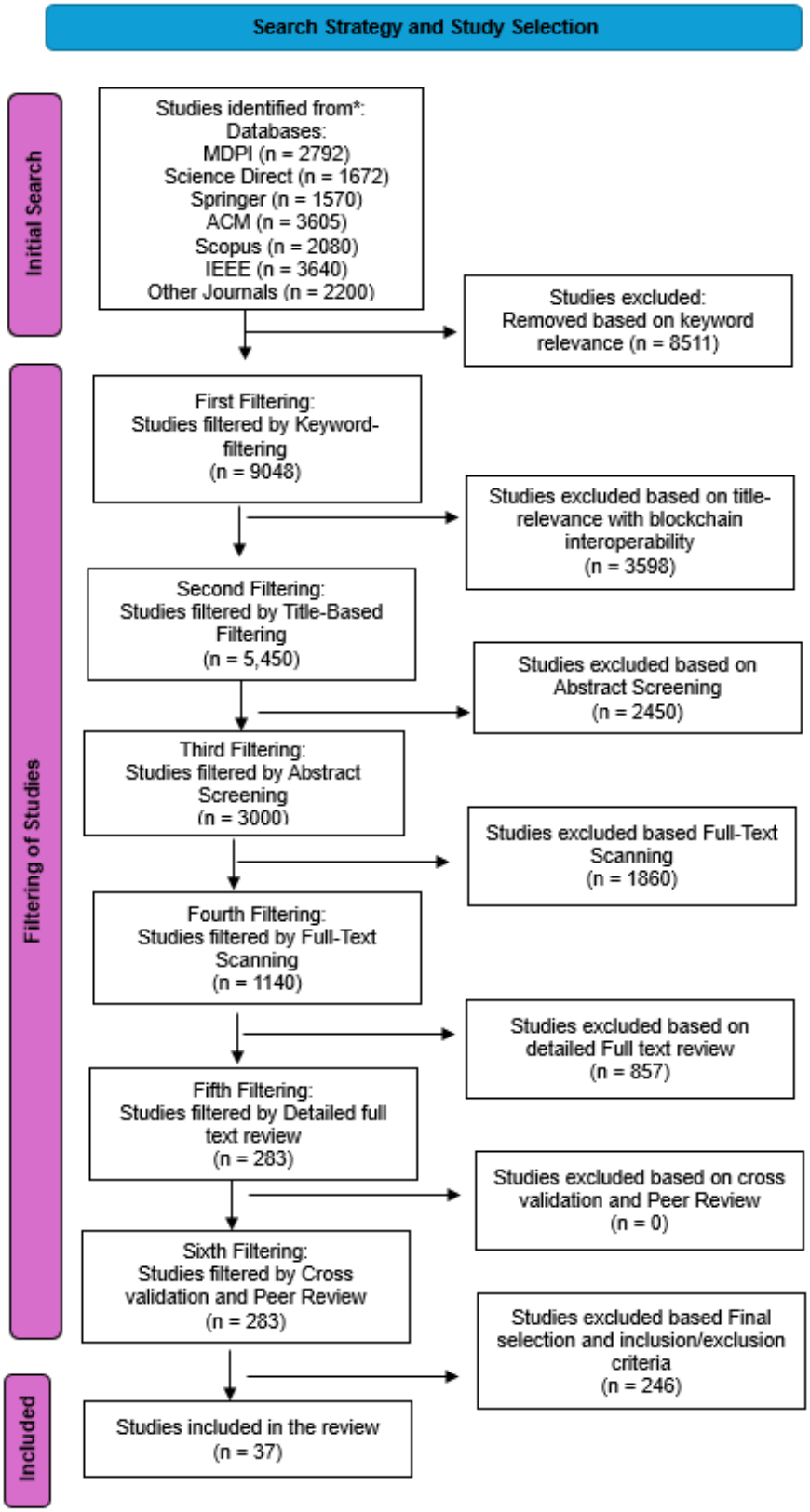
The studies excluded were unrelated, involved the repetition of research findings, offered no new insights, provided outdated information, were theoretical studies with no practical or experimental application, and were written in a language other than English.

3.4 Selected Studies

The research was concluded with a total of 37 studies in the conferred review article, as presented in the PRISMA flow chart.

3.5 Data Extraction and Analysis

Based on the PRISMA guidelines, studies were screened by the availability of information and qualitative data. Screening of relevant material was carried out making sure the availability of full text of articles and excluded if the title or abstract of the article didn't provide sufficient or relevant information. A qualitative analysis was carried out to identify the gaps and solutions in the relevant literature.


Search Strategy and Study Selection
Initial Search
Studies identified from*:
Databases:
MDPI (n = 2792)
Science Direct (n = 1672)
Springer (n = 1570)
ACM (n = 3605)
Scopus (n = 2080)
IEEE (n = 3640)
Other Journals (n = 2200)
Studies excluded:
Removed based on keyword relevance (n = 8511)
Filtering of Studies
First Filtering:
Studies filtered by Keyword-filtering
(n = 9048)
Studies excluded based on title-relevance with blockchain interoperability
(n = 3598)
Second Filtering:
Studies filtered by Title-Based Filtering
(n = 5,450)
Studies excluded based on Abstract Screening
(n = 2450)
Third Filtering:
Studies filtered by Abstract Screening
(n = 3000)
Studies excluded based Full-Text Scanning
(n = 1860)
Fourth Filtering:
Studies filtered by Full-Text Scanning
(n = 1140)
Studies excluded based on detailed Full text review
(n = 857)
Fifth Filtering:
Studies filtered by Detailed full text review
(n = 283)
Studies excluded based on cross validation and Peer Review
(n = 0)
Sixth Filtering:
Studies filtered by Cross validation and Peer Review
(n = 283)
Studies excluded based Final selection and inclusion/exclusion criteria
(n = 246)
Included
Studies included in the review
(n = 37)

4. RESULTS AND DISCUSSION

Blockchain interoperability has seen tremendous progress in decentralized systems, yet there remain prominent gaps that limit seamless integration and communication across platforms. The literature review identifies critical gaps in blockchain interoperability such as Standardization, Security, Scalability, and Governance.

The insufficiency of standardized protocols among blockchain platforms arises as a significant barrier. Every Blockchain has its unique consensus mechanisms, cryptographic protocols, and smart contract languages leading to an ecosystem of isolated "Value islands" [4]. Different blockchains employ varied consensus mechanisms and hinder the harmonized transaction validation processes. Having their strengths and weaknesses, consensus mechanisms pose a threat to smooth interoperability [42]. To mitigate this challenge several solutions such as middleware layer, cross-consensus bridging protocols, and hybrid consensus mechanisms are being developed and utilized [43, 44]. However, the attainment of a universal standard remains difficult. The absence of unified frameworks results in complexity among cross-chain interactions ultimately leading to insufficiencies and increased costs.

The inconsistency in smart contract languages and environments creates another barrier to cross-platform interactions. For a blockchain to utilize a smart contract on another chain we would need to rewrite and adapt the smart contract to the new language and environment, resulting in not only loss of time but also security vulnerabilities and a potential for errors. To address this, cross-chain smart contract platforms like Polkadot [15] and Cosmos [45] are being developed to support the interoperability of smart contracts across multiple chains. This standardization along with initiatives such as Blockchain Interoperability Alliance [46] and Transpiration techniques (Ethereum's EVM) [47] are aiming for shared foundations.

The promise of insurance of efficiency, privacy, and functionality by blockchain interoperability seems endangered by critical security and privacy concerns. Problems such as open exposure of data on a blockchain to anyone with access to critically endangered privacy. Solutions like cryptographic techniques namely Zero-knowledge proofs [34] and Homomorphic encryptions [48] are allowing improved and strict confidentiality. Trusted gateways in private blockchains and public blockchain interactions ensure the confidentiality of shared data for private chains [49]. Decentralized Identity solutions allow users to control their data and selectivity of sharing it across multiple blockchains. Empowering users with authority over their data and minimizing the risk of data breaches.

Governance structure plays a crucial role in ensuring the seamless integration of cross-chain communication. Existing blockchain ecosystems operate under different governance models, including on-chain governance (e.g., Polkadot's governance model) and off-chain governance (e.g., Bitcoin Improvement Proposals). However, these governance models create barriers to cross-chain transactions due to varying decision-making processes, stakeholder involvement, and upgrade mechanisms [11]. The lack of unified governance standards complicates interoperability, particularly in cases where conflicting protocol upgrades result in network fragmentation. A proposed governance framework for blockchain interoperability involves a multi-layer governance model that includes establishing common protocols for cross-chain communication (Protocol Standardization), Implementing smart contract-based governance to enable automated decision-making (Decentral-

ized Autonomous Governance) and ensuring that governance structures align with jurisdictional requirements while maintaining decentralization (Regulatory Compliance Adaptation).

Furthermore, scalability concerns in cross-chain interoperability mechanisms persist. Performance benchmarks such as transaction throughput, latency, and computational efficiency vary significantly among different solutions. For example, Polkadot's relay chain architecture achieves communication with a throughput of 1000 TPS, whereas Cosmos' IBC protocol supports up to 10,000 TPS under optimal conditions [24]. These metrics suggest that while interoperability solutions are improving, scalability remains an ongoing challenge that requires further optimization through sharding, state channels, and efficient consensus mechanisms.

There are significant regulatory and legal challenges, particularly in cross-border transactions where jurisdictional conflicts arise. Data privacy laws such as the General Data Protection Regulation (GDPR) impose strict requirements on data storage and transfer, which can hinder interoperability effects. Under GDPR, the right to be forgotten contradicts blockchain's immutability, raising concerns about compliance in cross-chain environments [39]. Additionally, financial regulations, including Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements, pose challenges for decentralized interoperability solutions. Platforms facilitating cross-chain asset transfer may be subject to multiple regulatory frameworks depending on the participating jurisdictions. For example, the Financial Action Task Force (FATF) guideline requires Virtual Asset Service Providers (VASPs) to adhere to stringent identity verification processes, potentially impacting decentralized bridges and trustless interoperability mechanisms [40].

A potential solution to regulatory challenges involves hybrid compliance mechanisms, such as Regulatory-Oriented Smart Contracts that embed compliance requirements directly into smart contracts to automate legal enforcement and Permissioned Interoperability frameworks that allow the implementation of permissioned cross-chain networks that comply with jurisdictional requirements while enabling selective data sharing. Legal concerns related to intellectual property, data sovereignty, and liability in decentralized environments also necessitate the development of standardized legal frameworks to ensure accountability in cross-chain transactions.

Applications for Blockchain Interoperability solutions across different sectors

Blockchain interoperability solutions enhance seamless data exchange and collaboration across various industries, fostering efficiency and security. TABLE 1 highlights key applications of blockchain interoperability in healthcare, education, supply chain, and other sectors, demonstrating its transformative potential.

Real-world implementations of blockchain interoperability provide insights into the feasibility and performance of existing solutions. For instance, a case study on the BSN Spartan Network demonstrates how blockchain interoperability can facilitate enterprise-grade applications across public and private blockchain networks. The Spartan Network employs hybrid connectors to enable seamless data exchange between Ethereum, Hyperledger Fabric, and Tezos, showcasing the viability of cross-chain interactions in financial and supply chain sectors [38].

Zero-knowledge proofs (ZKP) allow verification of the truth of statements between two parties without revealing additional information [50]. ZKPs play a crucial role in enhancing privacy and security. The integration of ZKP into healthcare sectors has seen some promising results. Al-Aswad

Table 1: Key Applications of Blockchain Interoperability in Healthcare, Education, Supply Chain, and Beyond

Author [Ref No]	Application Technique	Solution	Usage
Al-Aswad et al. [51]	Zero-Knowledge Proof (ZKP)	Age verification via trusted entity	Private medication verification
Tomaz et al. [52]	Zero-Knowledge Proof (ZKP)	Encrypted mHealth data sharing	Secure health data transmission
Tran et al. [53]	CrossCert Privacy-Focused Cross-Chain System	Anonymous credential checks	Verified educational credentials securely
Prasad et al. [54]	ZKP in Supply Chains	Confidential data	Compliant supply chain
Torongo and Torani [55]	Decentralized Identity Management (BDIMHS)	Interoperable authentication	Secure identity integration in healthcare
Zhang et al. [56]	IDRG (Data Rights Governance)	Privacy-preserving identity system	Controlled data access in metaverse apps
Qiao et al. [57]	Threshold Signatures	Secure group data interactions	Privacy in healthcare data sharing
Liu et al. [58]	Linkable Ring signatures	Ring signature for IoT and networks	Private micro-payments and smart cities
Hussain et al. [59]	Healthcare interoperability	Reduced duplicate clinical data	Cost-efficient healthcare management
Stewart et al. [60]	Healthcare Interoperability	Eliminated redundant procedures	Improved patient safety and efficiency

et al. developed a non-interactive ZKP to demonstrate the age of the person without revealing their exact age to the verifier with the help of a trusted entity accessed by both parties. By utilizing ZKP the private pharmacy was able to verify the medication report without affecting privacy or integrity. This blockchain decentralization system acted as a trusted party [51]. Tomaz et al. (2020) developed a lightweight Zero-Knowledge proof to be able to run on mHealth devices in which the health data is stored, transmitted, or shared shielded by Attribute-Based Encryption incorporating strictly controlled access and an end-to-end privacy guarantee [52].

In the education sector, verifying and validating credential information has always been a challenge of security, privacy, and interoperability. The CrossCert model developed by Tran et al. is a privacy-focused cross-chain system. Utilizing cryptographic proof (Zero-Knowledge proof) facilitates anonymous checks without compromising user details. This ensures security as well as maintaining ethical standards [53]. ZKPs improve privacy in supply chain transactions by verifying data integrity without revealing the actual information. This allows confidentiality while ensuring proof of compliance with specific standards or regulations [54].

The incorporation of blockchain-based identity management solutions (BDIMHS) is proving to be effective in providing secure, private, and scalable applications in the healthcare sector. BDIMHS, developed by Torongo and Torani (2023) is an example of supplementing interoperability in the form

of a rigorous standard identity management system that allows uninterrupted and secure exchange and integration of authentication among several healthcare setups. This model leverages heavily adopted identity W3C standards VC (Verifiable Credentials) and DIDs (Decentralized Identifiers) for the verified issuance of digital identity credentials [55]. With the growing popularity of metaverse applications, blockchain-based solutions provide secure and decentralized mechanisms to ensure privacy and data handling. A novel scheme IDRG (Identity-based Data Rights Governance) was developed by Zhang et al. (2024) contemplating privacy and data rights issues of the metaverse based on a privacy-preserving digital identity system. Techniques such as identity-based encryption, chameleon hash techniques, and proxy re-encryption were utilized to enhance throughput data rights management by having control over data and preservation of privacy policies along with a revocation mechanism allowing only authorized users to access and modify the data [56].

Ribiero et al. in a study utilized blockchain and smart contracts' strength within the context of MedClick. This led to healthcare applications based on smart contracts allowing the patients the possibility to safely store their health data along with interacting with their chosen health providers and professionals in one single platform [61]. The use of threshold signatures in improving security and privacy is of importance. In healthcare, the facilitation of dynamic data interaction could be achieved by using threshold group signatures [57]. Linkable ring signatures in vehicular networks and smart cities, for improving threshold computations in micropayments, a threshold (2,2) ECDSA can be utilized and identity-based ring signatures for general IoT [58]. Several other interoperability uses in healthcare include the chance of reducing duplicate chances in clinical systems such as laboratory reports, the cost of the system [59], and the improvement in the maturity of patient care by dropping disclosure to radioactivity actions [60].

These case studies provide empirical evidence of blockchain interoperability's transformative potential across multiple industries. However, further research is needed to standardize performance metrics and develop scalable, secure interoperability solutions that align with regulatory frameworks.

4.1 Study Limitations

This study identifies key limitations in the methodology, particularly regarding literature filtering and keyword-based selection, which may affect the findings' accuracy. Variations in terminology, keyword omissions, and polysemantic abbreviations may have excluded relevant studies, as blockchain interoperability research often lacks standardized terms. The absence of consistent vocabulary across the literature complicates automated filtering, increasing the risk of missing significant contributions that use unconventional jargons. Automated tools, while efficient, depend on linguistic patterns and metadata, potentially overlooking valuable studies if keywords do not match predefined criteria. Variations in titles and keywords may have led to the exclusion of influential papers using less conventional descriptors. Rapid innovation and diverse application contexts cause inconsistent terminology usage, complicating dataset completeness. Recognizing these limitations ensures a clearer interpretation of findings and supports ongoing methodological improvements in blockchain interoperability research.

4.2 Future Recommendations

This review lacks practical evaluations of the discussed mechanism, limiting the scope of theoretical insights. Future studies are directed towards focusing on standardizing interoperability protocols and attaining security vulnerabilities of blockchain bridges. Integration of blockchain with rising fields like IoT and AI should be emphasized to unlock novel cross-domain applications. Future studies should also focus on developing standardized blockchain interoperability terminology, expanding keyword strategies with synonyms and emerging terms, and combining automated and manual filtering to enhance accuracy and foster researcher collaboration for consistent frameworks.

5. CONCLUSION

Blockchain interoperability is pivotal for realizing the full potential of decentralized systems across industries. While mechanisms like HTLCs and blockchain bridges facilitate cross-chain communication, challenges related to scalability, security, and standardization persist. Cryptographic innovations such as Zero-Knowledge Proofs and Hybrid Connectors show promise in enhancing privacy, scalability, and seamless interactions. The study highlights the significant impact of interoperability in healthcare, education, and supply chain management, here secure, transparent data exchanges improve operational efficiency. However, gaps in governance frameworks and the absence of universal standards necessitate further research and development. Addressing these challenges can lead to more interconnected, efficient blockchain ecosystems, driving innovation and digital transformation across sectors.

6. CONFLICT OF INTEREST

None

7. ACKNOWLEDGMENT

None.

References

[1] Akanfe O, Lawong D, Rao HR. Blockchain Technology and Privacy Regulation: Reviewing Frictions and Synthesizing Opportunities. Int J Inf Manag. 2024;76:102753.

[2] Nakamoto S. Bitcoin: A Peer-To-Peer Electronic Cash System. Satoshi Nakamoto. 2008.

[3] Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Proj Yellow Pap. 2014:1-32.

[4] Wüst K, Gervais A. Do You Need a Blockchain? In: crypto valley conference on blockchain technology (CVCBT). IEEE. 2018.

[5] Cachin C. Architecture of the Hyperledger Blockchain Fabric. In: Workshop on distributed cryptocurrencies and consensus ledgers. Chicago.2016.

[6] Alhussayen AA, Jambi K, Khemakhem M, Eassa FE. A Blockchain Oracle Interoperability Technique for Permissioned Blockchain. IEEE Access. 2024.

[7] Puneeth RP, Parthasarathy G. Seamless Data Exchange: Advancing Healthcare With Cross-Chain Interoperability in Blockchain for Electronic Health Records. Int J Adv Comput Sci Appl. 2023;14.

[8] Yaga D, Mell P, Roby N, Scarfone K. Blockchain Technology Overview. 2019. ArXiv preprint: https://arxiv.org/pdf/1906.11078

[9] Zamyatin A, et al. Sok: Communication Across Distributed Ledgers. In: Financ Cryptogr Data Sec: 25th International Conference, FC 2021, Virtual Event. part II. Springer. 2021:3-36.

[10] Tate RV, Mane SB. A Framework for Interoperability in Blockchain Without Any Intermediaries. In: 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). IEEE. 2023:1-7.

[11] Belchior R, Vasconcelos A, Guerreiro S, Correia M. A Survey on Blockchain Interoperability: Past Present and Future Trends. ACM Comput Surv. 2021;54:1-41.

[12] https://polkadot.com/blog/polkadot-bridges-connecting-the-polkadot-ecosystem-with-external-networks

[13] Zamyatin A, Harz D, Lind J, Panayiotou P, Gervais A, et. al. Xclaim: Trustless Interoperable Cryptocurrency-Backed Assets. In: IEEE symposium on security and privacy (SP). IEEE. 2019:193-210.

[14] Bentov I, Ji Y, Zhang F, Breidenbach L, Daian P, et. al. Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware. In: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. New York USA: ACM. 2019:1521-1538.

[15] Ren K, Ho NM, Loghin D, Nguyen TT, Ooi BC, et. al. Interoperability in Blockchain: A Survey. IEEE Trans Knowl Data Eng. 2023;35:12750-12769.

[16] Wood G. Polka Dot: Vision for a Heterogeneous Multi-Chain Framework. 2016;21:4662.

[17] Eberhardt J, Tai S. On or off the Blockchain? Insights on off-chaining computation and data. In: Serv-Oriented Cloud Comput: 6th IFIP WG 2.14 European Conference ESOCC Oslo Norway. Springer. 2017:3-15.

[18] Taherdoost H. Smart Contracts in Blockchain Technology: A Critical Review. Information. 2023;14:117.

[19] Sklaroff JM. Smart Contracts and the Cost of Inflexibility. Univ Pa L Rev. 2017;166:263.

[20] Esposito C, De Santis A, Tortora G, Chang H, Choo KK. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 2018;5:31-37.

[21] Hackius N, Petersen M. Blockchain in Logistics and Supply Chain: Trick or Treat? In: Digitalization in supply chain management and logistics: smart and digital solutions for an Industry 4.0 environment. Proceedings of the Hamburg international conference of logistics (HICL). 2017;23:3-18.

[22] Zhang X. Blockchain Technology in Various Fields: Applications Challenges and Future. Highlights Sci Eng Technol. 2023;57:154-160.

[23] Lutfiani N, Harahap EP, Aini Q, Ahmad AD, Rahardja U. Inovasi Manajemen Proyek I-Learning Menggunakan Metode Agile Scrumban. InfoTekJar J Nas Inform dan Teknol Jar. 2020;5:96-101.

[24] https://cosmos.network/ibc/

[25] Mohanty D, Anand D, Aljahdali HM, Villar SG. Blockchain Interoperability: Towards a Sustainable Payment System. Sustainability. 2022;14:913.

[26] Alhussayen A, Jambi K, Eassa F, Khemakhem M. Performance Evaluation of an Oracle-Based Interoperability for Permissioned Blockchain. Computing. 2024;106:3627-3655.

[27] Khan S, Amin MB, Azar AT, Aslam S. Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability. IEEE Access. 2021;9:116672-116691.

[28] Wang G. Sok: Exploring Blockchains Interoperability. Cryptol Eprint Arch. 2021.

[29] https://blockstream. com/assets/downloads/pdf/liquid-whitepaper.pdf

[30] Li J, Zhao W. Blockchain Cross-Chain Protocol Based on Improved Hashed Time-Locked Contract. Clust Comput. 2024;27:12007-12027.

[31] Li N, Qi M, Xu Z, Zhu X, Zhou W, et. al. Blockchain Cross-Chain Bridge Security: Challenges Solutions and Future Outlook. Distrib Ledger Technol Res Pract. 2024;4:1-34.

[32] Li W, Bu J, Li X, Chen X. Security Analysis of Defi: Vulnerabilities Attacks and Advances. In: IEEE International Conference on Blockchain (Blockchain). IEEE. 2022:488-493.

[33] https://ibcprotocol.org/documentation/.

[34] Sun X, Yu FR, Zhang P, Sun Z, Xie W, et. al. A Survey on Zero-Knowledge Proof in Blockchain. IEEE Netw. 2021;35:198-205.

[35] Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements Challenges and Opportunities. J Inf Sec Appl. 2024;80:103678.

[36] Baird L, Garg S, Jain A, Mukherjee P, Sinha R, et. al. Threshold Signatures in the Multiverse. In: IEEE Symposium on Security and Privacy (SP). IEEE. 2023:1445-1470.

[37] Padmavathi U, S HR, Jayashre N, Gummaraju N. Examining Architectural Aspects of Hyperledger Fabric: A Thorough Review. In: IEEE International Conference on Innovations and Challenges in Emerging Technologies (ICICET). 2024:1-6.

[38] Lai Y, Yang J, Liu M, Li Y, Li S. WEB3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. Blockchains. 2023;1:111-131.

[39] Harris CG. Cross-Chain Technologies: Challenges and Opportunties for Blockchain Interoperability. In: IEEE International Conference on Omni-layer Intelligent Systems (COINS). IEEE. 2023.

[40] Zhao Q, et al. A Comprehensive Overview of Security Vulnerability Penetration Methods in Blockchain Cross-Chain Bridges. Authorea Prepr. 2023.

[41] Sanka AI, Cheung RC. A Systematic Review of Blockchain Scalability: Issues, Solutions, Analysis and Future Research. J Netw Comput Appl. 2021;195:103232.

[42] Lohachab A, Garg S, Kang B, Amin MB, Lee J, et al. Towards Interconnected Blockchains: A Comprehensive Review of the Role of Interoperability Among Disparate Blockchains. ACM Comput Surv. 2021;54:1-39.

[43] Bhatia R. Interoperability Solutions for Blockchain. In: 2020 international conference on smart technologies in computing, electrical and electronics (ICSTCEE). IEEE; 2020.

[44] Lashkari B, Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms. IEEE Access. 2021;9:43620-43652.

[45] Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access. 2016;4:2292-2303.

[46] https://capuana.ifi.uzh.ch/publications/PDFs/17668_Master_Thesis_Timo_Hegnauer.pdf

[47] Dhillon V, Metcalf D, Hooper M. Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You. Apress. 2021.

[48] Albrecht M, Chase M, Chen H, Ding J, Goldwasser S, et al. Homomorphic Encryption Standard. In: Lauter K, Dai W, Laine K, editors. Protecting privacy through homomorphic encryption. Cham: Springer International Publishing. 2021:31-62.

[49] https://www.weforum.org/publications/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction/

[50] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges. IEEE Commun Surv Tutorials. 2020;22:2521-2549.

[51] Al-Aswad H, Hasan H, Elmedany W, Ali M, Balakrishna C. Towards a Blockchain-Based Zero-Knowledge Model for Secure Data Sharing and Access. In: 7th International conference on future internet of things and cloud workshops (FiCloudW). IEEE. 2019.

[52] Tomaz AE, Nascimento JC, Hafid AS, De Souza JN. Preserving Privacy in Mobile Health Systems Using Non-interactive Zero-knowledge Proof and Blockchain. IEEE Access. 2020;8:204441-204458.

[53] Tran TD, Minh PK, Thuy TLT, Duy PT, Cam NT, et al. Crosscert: A Privacy-Preserving Cross-Chain System for Educational Credential Verification Using Zero-Knowledge Proof. In: International Conference on Industrial Networks and Intelligent Systems. Springer. 2024.

[54] Prasad S, Tiwari N, Chawla M, Tomar DS. Zero-Knowledge Proofs in Blockchain-Enabled Supply Chain Management. In: Kumar A, Ahuja NJ, Kaushik K, Tomar DS, Khan SB, editors. Sustainable security practices using blockchain, quantum and post-quantum technologies for real time applications. Springer. 2024:47-70.

[55] Torongo AA, Toorani M. Blockchain-based Decentralized Identity Management for Healthcare Systems. 2023. ArXiv preprint: https://arxiv.org/pdf/2307.16239

[56] Zhang C, Zhao M, Zhang W, Fan Q, Ni J, et al. Privacy-Preserving Identity-Based Data Rights Governance for Blockchain Empowered Human-Centric Metaverse Communications. IEEE J Sel Areas Commun. 2024;42:963-977.

[57] Qiao R, Luo XY, Zhu SF, Liu AD, Yan XQ, et al. Dynamic Autonomous Cross Consortium Chain Mechanism in E-healthcare. IEEE J Biomed Health Inform. 2020;24:2157-2168.

[58] Liu H, Han D, Cui M, Li KC, Souri A, et al. Idenmultisig: Identity-Based Decentralized Multi-Signature in Internet of Things. IEEE Trans Comp Soc Syst. 2023;10:1711-1721.

[59] HHussain S, Rahman H, Abdulsaheb GM, Al-Khawaja H, Khalaf OI. A Blockchain-Based Approach for Healthcare Data Interoperability. Int J Adv Soft Comput Appl. 2023;15.

[60] Stewart BA, Fernandes S, Rodriguez-Huertas E, Landzberg M. A Preliminary Look At Duplicate Testing Associated With Lack of Electronic Health Record Interoperability for Transferred Patients. J Am Med Inform Assoc. 2010;17:341-344.

[61] da Fonseca Ribeiro MI, Vasconcelos A. MedBlock: Using Blockchain in Health Healthcare Application Based on Blockchain and Smart Contracts. ICEIS. 2020;1.