Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.070413

REVIEW

Security and Privacy in Permissioned Blockchain Interoperability: A Systematic Review

Alsoudi Dua[1], Tan Fong Ang[1], Chin Soon Ku[2,*], Okmi Mohammed[1,3], Yu Luo[4], Jiahui Chen[4], Uzair Aslam Bhatti[5] and Lip Yee Por[1,*]

[1]Center of Research for Cyber Security and Network (CSNET), Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia
[2]Department of Computer Science, Universiti Tunku Abdul Rahman, Kampar, 31900, Malaysia
[3]Department of Information Technology and Security, Jazan University, Jizan, 45142, Saudi Arabia
[4]School of Computer Science and Technology, Guangdong University of Technology, Guangzhou, 510006, China
[5]School of Information and Communication Engineering, Hainan University, Haikou, 570228, China

*Corresponding Authors: Chin Soon Ku. Email: kucs@utar.edu.my; Lip Yee Por. Email: porlip@um.edu.my

Received: 15 July 2025; Accepted: 19 August 2025; Published: 23 September 2025

ABSTRACT: Blockchain interoperability enables seamless communication and asset transfer across isolated permissioned blockchain systems, but it introduces significant security and privacy vulnerabilities. This review aims to systematically assess the security and privacy landscape of interoperability protocols for permissioned blockchains, identifying key properties, attack vectors, and countermeasures. Using PRISMA 2020 guidelines, we analysed 56 peer-reviewed studies published between 2020 and 2025, retrieved from Scopus, ScienceDirect, Web of Science, and IEEE Xplore. The review focused on interoperability protocols for permissioned blockchains with security and privacy analyses, including only English-language journal articles and conference proceedings. Risk of bias in the included studies was assessed using the MMAT. Methods for presenting and synthesizing results included descriptive analysis, bibliometric analysis, and content analysis, with findings organized into tables, charts, and comparative summaries. The review classifies interoperability protocols into relay, sidechain, notary scheme, HTLC, and hybrid types and identifies 18 security and privacy properties along with 31 known attack types. Relay-based protocols showed the broadest security coverage, while HTLC and notary schemes demonstrated significant security gaps. Notably, 93% of studies examined fewer than four properties or attack types, indicating a fragmented research landscape. The review identifies underexplored areas such as ACID properties, decentralization, and cross-chain attack resilience. It further highlights effective countermeasures, including cryptographic techniques, trusted execution environments, zero-knowledge proofs, and decentralized identity schemes. The findings suggest that despite growing adoption, current interoperability protocols lack comprehensive security evaluations. More holistic research is needed to ensure the resilience, trustworthiness, and scalability of cross-chain operations in permissioned blockchain ecosystems.

KEYWORDS: Blockchain; security; privacy; attack; threat; interoperability; cross-chain

1 Introduction

Blockchain technology has revolutionized decentralized systems by providing distributed, transparent, and tamper-resistant ledgers [1]. Among its variants, permissioned blockchains have gained significant traction in enterprise and institutional environments where access control, confidentiality, and regulatory compliance are crucial [2]. As organizations increasingly adopt blockchain solutions tailored to domains, such as the Internet of Things (IoT) [3–5], vehicular [6], and healthcare [7], the need for secure and efficient interoperability between these systems has become both urgent and inevitable [8]. Interoperability protocols act as bridges, enabling data exchange, asset transfers, and smart contract execution across otherwise isolated blockchain networks [9].

However, the integration of interoperability protocols introduces a new attack surface, exposing systems to sophisticated security and privacy threats. Since May 2021, cross-chain transaction attacks have caused losses exceeding USD 3.1 billion [10]. Existing surveys generally address only a narrow scope of security analyses. Their focus is often limited to a small set of countermeasures [9,11]. Others focus solely on specific attack types or security and privacy attributes [12–14]. Many also concentrate predominantly on cross-chain protocols in permissionless blockchain environments [15–17]. Consequently, no comprehensive and systematic review currently addresses the security and privacy challenges specific to permissioned blockchain interoperability. The absence of such a holistic analysis poses significant difficulties for system architects and developers seeking to secure interoperability protocols against evolving threats.

To address this gap, this study conducts a systematic literature review (SLR) that synthesizes the security properties, privacy considerations, threats, and countermeasures of interoperability protocols in permissioned blockchains. The methodology follows the PRISMA 2020 guidelines [18], which include a flow diagram and 27-item checklist to ensure transparent and comprehensive reporting of systematic reviews. A PRISMA flow diagram is used to illustrate the study selection process. Furthermore, the Mixed Methods Appraisal Tool (MMAT) [19], a well-established instrument for assessing the methodological quality of mixed-method, quantitative, and qualitative studies, was applied to evaluate the included research. Both the PRISMA checklist and MMAT-based quality assessment are provided in the supplementary materials to enhance transparency and reproducibility. This review offers a structured and in-depth analysis of existing work while identifying key gaps in current research and providing insights to guide future development.

Understanding and mitigating these challenges is critical for safeguarding the growing investments in blockchain-based applications. Robust security and privacy analysis are essential to ensure the trustworthiness, resilience, and scalability of interoperability mechanisms in permissioned blockchain ecosystems [10].

This article is organized as follows. Section 2 presents the foundational concepts of blockchain technology, interoperability protocols, and related work, while Section 3 describes the research methodology, including the systematic review protocol, research questions, and study selection criteria. Section 4 provides the review results following the PRISMA 2020 framework, covering study selection, quality assessment, publication trends, and study characteristics, as well as analyses of security and privacy properties (Section 4.5), attack types (Section 4.6), and countermeasures (Section 4.7), which collectively address the research questions. It also discusses heterogeneity among studies (Section 4.8) and reporting bias (Section 4.9). Section 5 critically examines the findings, highlighting research gaps (Section 5.1) and future directions (Section 5.2), and Section 6 concludes with key insights and implications.

2 Background

This section provides background about Blockchain technology and interoperability protocols.

2.1 Blockchain

Blockchain technology comprises several core components that collectively ensure decentralization, security, and immutability [20]. At its foundation, the distributed ledger maintains a chronological chain of cryptographically linked blocks, ensuring that any modification to a past record is immediately detectable [21]. Consensus algorithms, including variants like Proof of Work (PoW) and Proof of Stake

(PoS), allow participants to collaboratively verify transactions without relying on a central authority [22]. Cryptographic primitives underpin blockchain security; for example, hash functions generate unique digital fingerprints of data, ensuring integrity, while advanced cryptographic methods, such as zero-knowledge proofs, enable a participant to demonstrate that they possess valid information without disclosing the information itself, thereby supporting privacy-preserving cross-chain transactions [23]. Smart contracts are autonomous programs deployed on the blockchain that execute predefined agreements automatically when specified conditions are met, minimizing the need for intermediaries and promoting trustless interaction [22]. Collectively, these components create a tamper-evident, auditable, and trustless framework for decentralized systems [24–26]. Blockchain has been applied across diverse domains, including IoT [3–5], vehicular networks [6], and healthcare [7].

Since the introduction of Bitcoin, numerous blockchain platforms have been developed, including Ethereum [20] and Hyperledger Fabric [27,28]. Depending on the participant access permissions, intended application scenarios, and degree of decentralization, blockchain systems are broadly categorized into two types: permissionless and permissioned [29].

Fig. 1 provides an overview of blockchain categories. Permissionless blockchains (e.g., Bitcoin and Ethereum) are public networks that allow any user to join, leave, and view transactions, often anonymously. In contrast, permissioned blockchains restrict participation to authorized nodes, offering an additional layer of control and security. These are further divided into consortium blockchains, where access is limited to a group of trusted organizations [29], and private blockchains, where a single entity governs participation and enforces strict access restrictions [29].

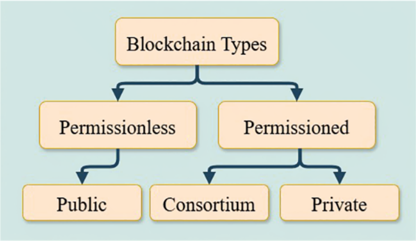


Figure 1: Categories of blockchain networks

To address enterprise-specific requirements, several notable permissioned blockchain frameworks have been introduced. Among them, Hyperledger Fabric offers a modular architecture tailored for business networks. Originally built on a Byzantine fault-tolerant consensus algorithm, Fabric now supports alternative consensus mechanisms to accommodate diverse enterprise needs [27,28]. Quorum, developed by JP Morgan as a fork of Ethereum, introduces key modifications such as permissioned participation, enhanced transaction privacy, a novel consensus mechanism, and reduced transaction fees, making it particularly suitable for financial and enterprise-grade applications [30]. Another prominent framework, Corda by R3, is a semi-open-source platform widely recognized in the financial sector. Unlike conventional blockchains, Corda employs a notary pool to achieve consensus, reflecting its focus on transaction verification and privacy in regulated industries [31]. Similarly, Multichain provides a flexible platform for deploying customized permissioned blockchains, emphasizing simplicity, privacy, and scalability across a wide range of business domains [32].

2.2 Interoperability Protocols

Interoperability refers to the capacity of different blockchains—whether public, private, or consortium-based—to seamlessly exchange assets, share data, and execute smart contracts without requiring modifications to their underlying infrastructure [9]. This capability is essential for preventing ecosystem fragmentation, supporting diverse application scenarios, and enabling broader adoption of blockchain technology across real-world domains. To meet the requirements of modern use cases, interoperability must extend beyond simple asset transfers or event notifications to include the secure and efficient exchange of arbitrary data. Such functionality is critical for applications that require privacy-preserving data sharing, regulatory compliance, and automated business workflows. For instance, asset transfer involves securely moving tokens or digital assets between distinct blockchain networks, while asset exchange entails transferring ownership of assets between users on different chains [16]. Arbitrary data sharing is particularly important in real-world scenarios, such as supply chain management or healthcare, where complex data structures must be transferred with guaranteed integrity, confidentiality, and cross-chain compatibility [33]. Smart contract invocation further extends interoperability by allowing one blockchain to trigger and receive responses from a smart contract deployed on another chain [16]. Collectively, these capabilities enhance enterprise integration, foster innovation, and ensure that blockchain solutions can meet both organizational and decentralized application (DApp) requirements.

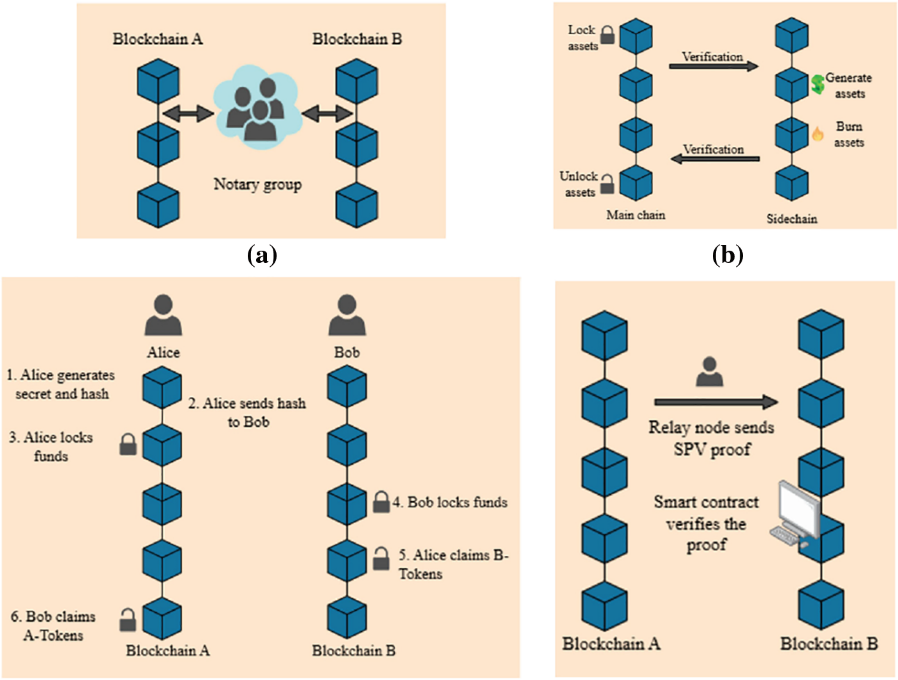
Interoperability protocols expand the foundational blockchain architecture by incorporating key components that enable secure cross-chain communication. Consensus mechanisms are used to validate and finalize transactions across multiple chains, while cryptographic primitives such as hash locks, digital signatures, and multi-signature schemes ensure trustless execution [34]. Incentive mechanisms are often integrated to align the behavior of participants with the security and performance objectives of the protocol. In addition, application interfaces are designed to allow DApps to perform cross-chain operations such as asset transfers, data sharing, and smart contract invocations in a seamless manner [12].

The classification of interoperability mechanisms varies among researchers. Buterin [20] identified three primary categories: notary schemes, sidechains or relays, and HTLCs. Another study [9] extended this classification to include blockchain-agnostic protocols, while Yin et al. (2023) proposed four categories: notary schemes, HTLCs, sidechains, and hybrid technologies [16]. Other works follow a simplified taxonomy that includes notary schemes, sidechains or relays, and HTLCs [11,13].

In this review, interoperability protocols are categorized into five key mechanisms: sidechains, relays, HTLCs, notary schemes, and hybrid approaches. Fig. 2 illustrates the first four mechanisms, where subfigure (a) depicts a notary scheme relying on a trusted intermediary or federation to confirm cross-chain events, subfigure (b) shows a sidechain mechanism that uses an auxiliary blockchain with its own consensus to facilitate secure asset movements, subfigure (c) presents an HTLC-based protocol that employs cryptographic conditions (hash locks and time locks) to enable trustless atomic swaps, and subfigure (d) demonstrates a relay-based mechanism that maintains a light client or verification contract on one chain to monitor and validate the state of another chain.

Although hybrid mechanisms combine elements of sidechains, relays, HTLCs, and notary schemes, they are best understood as overarching conceptual frameworks rather than standalone implementations. Therefore, to avoid redundancy with the visual representations of the individual mechanisms, we provide a textual explanation of hybrid mechanisms instead of an additional diagram. The following paragraphs offer a concise overview of each interoperability mechanism:

- Sidechains operate as independent blockchains connected to a mainchain, often via a two-way peg, which enables the secure locking and unlocking of assets across the chain. Each sidechain maintains its own ledger and consensus algorithm while being capable of verifying events on the mainchain [20].
- Relays allow one blockchain to verify the state or events of another by maintaining a light client or simplified payment verification (SPV) proof of the external chain. Relay nodes facilitate this interaction, sometimes extending into more complex relay chains that act as hubs for multichain communication [20].
- Notary schemes rely on a centralized or federated group of trusted parties to confirm the occurrence of an event on one chain and relay it to another. While simple and efficient, this method introduces trust assumptions that may weaken decentralization [20].
- HTLCs implement trustless atomic swaps by ensuring that a transaction on one chain only completes if a corresponding transaction on another chain does so within a specified time window. This method eliminates the need for intermediaries and enforces atomicity in cross-chain operations [20].
- Hybrid interoperability mechanisms combine features of multiple approaches—such as sidechains, relays, HTLCs, and notary schemes—to leverage their strengths while mitigating individual limitations. For example, a hybrid mechanism may use a relay-based architecture for continuous state verification, HTLCs for trustless atomic swaps, and notary-based validators to ensure cross-chain authenticity [12].



(a) (b)

(c) (d)

Figure 2: Interoperability Mechanisms in Blockchain Networks: (**a**) Notary scheme, which relies on a trusted intermediary or a group of entities to validate and relay cross-chain events; (**b**) Sidechain mechanism, which uses an auxiliary blockchain with its own consensus algorithm to facilitate secure asset transfers and data exchange; (**c**) Hashed Time-Lock Contract (HTLC) mechanism, which employs cryptographic hash locks and time constraints to enable trustless atomic swaps between chains; (**d**) Relay-based mechanism, which uses a light client or verification contract to track and validate the state of another blockchain

Several blockchain interoperability protocols have been deployed in real-world settings, demonstrating both practical utility and growing adoption. Cosmos enables communication and asset transfers among independent blockchains via the Inter-Blockchain Communication (IBC) protocol. Cosmos supports modular, sovereign blockchain development and can link private or consortium networks, addressing scalability and interoperability limits of traditional monolithic chains [35]. Polkadot connects heterogeneous blockchains through a central relay chain, offering shared security while preserving each chain's unique logic and consensus. Developed with the Substrate framework, it supports cross-chain communication, token transfers, and governance adaptable for both public and enterprise contexts [36]. Quant Overledger serves as a middleware layer for interoperability between existing permissioned and permissionless networks. Rather than creating new blockchains, it focuses on compliance, enterprise integration, and abstraction of blockchain complexity, making it well-suited for regulated environments [37]. In decentralized finance (DeFi), THORChain—built on the Cosmos SDK—enables direct asset exchanges across blockchains without wrapped tokens or centralized exchanges. Using its native token RUNE and continuous liquidity pools, it offers lessons in secure cross-chain asset transfer relevant to both open and permissioned ecosystems [38].

2.3 Related Works

The increasing vulnerabilities of interoperability protocols in permissioned blockchains underscore the urgent need for systematic evaluations of their security and privacy properties, associated attack vectors, and corresponding countermeasures. Although several studies have explored specific security challenges, the literature still lacks a unified and comprehensive review that synthesizes the various security properties, privacy considerations, threats, and defense mechanisms within the context of permissioned blockchain interoperability.

For instance, the study by [9] identifies four fundamental properties—atomicity, safety, liveness, and decentralization—highlighting their role in ensuring secure cross-chain operations. Building upon this foundation, study [11] investigates design trade-offs between properties such as atomicity, integrity, and availability, particularly in relation to consensus mechanisms.

Subsequent research has expanded the scope of analysis. In [12], the authors introduce extended security properties, including fairness, verifiability, and freshness, while enhancing privacy protection through techniques such as unlinkability and indistinguishability. Similarly, study [13] offers a systematic review of functional properties (e.g., atomicity and finality) and attack resilience, focusing on measures such as double-spending prevention and mitigation of Denial of Service (DoS) attacks, alongside the incorporation of advanced privacy-preserving techniques.

In [14], the emphasis shifts towards fault tolerance and real-world vulnerability mitigation, providing practical insights into deployment challenges. Building on this foundation, study [15] formalizes a structured evaluation framework by distinguishing between security properties (e.g., integrity and accountability) and privacy properties (e.g., anonymity and confidentiality), thereby offering a more holistic perspective on cross-chain security.

More recent studies have further refined these concepts. For example, study [16] operationalizes reliability through three critical dimensions: fairness, atomicity, and fault tolerance. The same work also highlights privacy properties, including confidentiality, anonymity, and unlinkability, as essential elements of robust interoperability protocols. Additionally, study [17] applies a well-established computer science paradigm by adopting the Atomicity, Consistency, Isolation, and Durability (ACID) model. The ACID model outlines fundamental properties for reliable transaction processing, ensuring that transactions are executed as indivisible units, maintain data integrity, operate independently of concurrent processes, and remain permanently recorded once completed. Within the context of blockchain, these principles form the basis for designing secure and consistent cross-chain operations [17].

To contextualize this review in the broader research landscape, Table 1 summarizes prior surveys on blockchain security, privacy, and attack countermeasures. The table compares these studies based on their focus on permissioned blockchains (PB), the number of security and privacy properties (NSPP) and attack types (NA) identified, as well as their discussions of countermeasures (C), research gaps (G), and future directions (FD). It also provides the publication year range of the reviewed papers, offering a clear comparison of scope and coverage.

Table 1: Summary of existing surveys on security, privacy, and attack countermeasures in blockchains

Ref.	PB	NSPP	NA	C	G	FD	Year
[9]	Limited	4	2	Limited	Yes	Limited	2014–2023
[11]	Limited	6	0	Limited	Yes	Limited	2018–2022
[12]	Limited	12	4	Yes	Yes	Yes	2014–2022
[13]	Limited	12	13	Yes	Yes	Yes	2016–2021
[14]	Limited	11	20	Yes	Yes	Yes	2012–2023
[15]	No	4	0	Limited	Limited	Limited	2017–2024
[16]	No	12	3	Limited	Yes	Limited	2018–2023
[17]	No	11	5	Limited	Limited	Limited	2014–2024
This work	Yes	18	31	Yes	Yes	Yes	2020–2025

Note: Ref.: Reference; PB: focus on permissioned blockchains; NSPP: Number of security and privacy properties identified; NA: Number of attacks identified; C: Countermeasures Identified; G: Gaps identified; FD: Future directions provided; Year: Year Range of Reviewed Papers.

Despite these contributions, most existing surveys concentrate on a narrow subset of attacks, security properties, privacy features, and countermeasures within blockchain interoperability architectures. This study addresses these gaps by conducting an SLR aligned with the PRISMA guidelines [18]. To the best of our knowledge, this work is the first comprehensive review to examine a broad spectrum of security and privacy properties, attack vectors, and defense mechanisms, while simultaneously identifying research gaps and inconsistencies in current security analyses.

3 Methods

In this section, the methodology used to conduct the SLR is described. The objective of the SLR is to review the security and privacy analysis guidelines for interoperability protocols across permissioned blockchains. Based on the PRISMA 2020 guidelines (see S1 File: PRISMA 2020 checklist), the review process was organized to ensure a standardized and transparent approach to study selection, data extraction, and reporting. This review was not registered, as protocol registration is not typically required in computer science research.

The PRISMA guidelines comprise a 27-item checklist and a three-phase flow diagram, which collectively facilitate transparent reporting of the processes used to identify, screen, and select studies for inclusion. The study selection process entails an involved description of the search strategy and the specific scholarly databases used to retrieve the studies. Hence, identification, screening, and inclusion were implemented during the study selection process. During the identification phase, we conducted a systematic search of four scholarly databases using predefined keywords associated with blockchain interoperability, privacy, and security. In the screening phase, studies that did not correlate with the review objectives were excluded based on the titles and abstracts. In order to evaluate the methodological quality and relevance of the remaining studies to the research scope, the articles were evaluated in accordance with inclusion and exclusion criteria to ascertain their inclusion.

All phases of the study selection process were conducted independently by two reviewers in order to reduce bias and improve reliability. The consensus discussions that were conducted during this process were used to resolve any disagreements that arose, with the assistance of a third reviewer when necessary.

3.1 Research Questions

This review is guided by the following research questions (RQs):

- What are the existing security and privacy properties of interoperability protocols across permissioned blockchains?
- What are the specific attacks associated with interoperability protocols in these environments?
- What countermeasures have been proposed to preserve the security and privacy of such protocols?

Aligned with these questions, the primary objectives of this study are to:

- Identify the security and privacy properties relevant to interoperability protocols.
- Investigate the attack types targeting these protocols and their implications.
- Analyze the proposed countermeasures, including their effectiveness and limitations.

To demonstrate the alignment between research questions and the study's structure, Table 2 maps the RQs to their respective sections and summarizes how each is addressed. Specifically, RQ1 consolidates 18 identified security and privacy properties across interoperability protocols (Section 4.5), RQ2 examines 31 documented attack types and their relevance (Section 4.6), and RQ3 identifies defensive strategies and mitigation mechanisms designed to ensure security and privacy (Section 4.7).

Table 2: Mapping of research questions (RQs) to study sections and key contributions

Research question	Presented in	Brief description of how the RQ is addressed
RQ1: What are the existing security and privacy properties of interoperability protocols across permissioned blockchains?	4.5 Security and Privacy Properties	Synthesizes 18 identified properties and highlights their coverage across various interoperability mechanisms.
RQ2: What are the specific attacks associated with interoperability protocols in these environments?	4.6 Attack Types	Analyzes 31 attack types, including their frequency and relevance to different protocol categories.
RQ3: What countermeasures have been proposed to preserve the security and privacy of such protocols?	4.7 Countermeasures (Sections 4.7.1 Countermeasures to Maintain Security and Privacy Properties and 4.7.2 Countermeasures to Prevent Attacks)	Summarizes defensive strategies and their effectiveness in maintaining security and privacy.

3.2 Identifying Information Sources/Databases

In the article searching process, Gusenbauer and Haddaway [39] suggested 14 databases that could serve as the leading databases. Among them, we selected four scholarly databases: Scopus, ScienceDirect, Web of Science, and IEEE Xplore, focusing on studies related to blockchain interoperability protocols.

Google Scholar is widely recognized as one of the world's most popular databases. Due to several problems and shortcomings, this database cannot be used as the primary database for SLR [39].

The search was performed in all fields, without any filter, using terms related to blockchain interoperability, permissioned blockchains, security and privacy, and cross-chain attacks. The final search was conducted in May 2025.

3.3 Developing the Search Strategy/Search Terms

We performed a search methodology that complies with the research objectives and questions of this review paper. This methodology combines keywords and a regulated vocabulary, employing Boolean operators (e.g., AND, OR) to refine the search queries based on the syntax requirements of each database. In addition, to ensure that only relevant studies were included, two essential terms, "blockchain interoperability" and "security/privacy," were employed as guiding criteria. The final search string employed was as follows:

("blockchain" AND ("security" OR "privacy") AND ("attack" OR "threat") AND ("interoperability" OR "cross-chain" OR "cross-blockchain")).

This search string was originally utilized for title abstracts and keywords across scholarly databases. Nevertheless, we noted that some relevant studies excluded these essential terms from their abstracts and/or keyword sections. Consequently, we expanded the search to encompass each paper's full text and metadata, including the abstract, title, and keywords. Manual screening of the full text was required in several cases. While this process was considerably time-consuming and labor-intensive, it was necessary to avoid excluding important studies that might otherwise have been missed.

3.4 Inclusion and Exclusion Criteria

We established inclusion and exclusion criteria to determine which studies would be accepted into the review and which would be excluded. The specific criteria used in this review are summarized in Table 3, which outlines the inclusion and exclusion conditions applied during the study selection process.

Table 3: Inclusion and exclusion criteria applied in study selection

Inclusion criteria (IC)	Exclusion criteria (EC)
IC1: Paper focuses on interoperability protocols.	EC1: Paper does not focus on interoperability protocols.
IC2: Paper applies to permissioned blockchains.	EC2: Paper does not apply to permissioned blockchains.
IC3: Paper includes security and privacy analyses.	EC3: Paper does not include security and privacy analyses.
IC4: Paper published between 2020 and 2025.	EC4: Paper published before 2020.
IC5: Peer-reviewed papers, articles, or conference proceedings.	EC5: Review papers, survey papers, or grey literature.
IC6: Paper published in English.	EC6: Paper not published in English.

This review focuses on literature published between 1st January 2020 and 31st December 2025 to capture the most recent advancements in blockchain interoperability, a field that has evolved rapidly with the emergence of cross-chain protocols, DeFi, and enterprise-oriented applications [40,41]. Limiting the primary scope to this timeframe ensures both focus and relevance [42]; however, we also recognize the importance of early foundational contributions that continue to influence current research and implementation trends.

Buterin's seminal work defined the core categories of cross-chain protocols—notary schemes, sidechains/relays, and HTLCs—which remain fundamental to interoperability studies [20]. Early initiatives such as Cosmos [35] and Polkadot [36] introduced hub-and-relay architectures to enable native multi-chain interoperability, while middleware solutions like Quant Overledger [37] and cross-chain liquidity protocols such as THORChain [38] expanded on these principles to address practical challenges of asset transfer and data exchange across heterogeneous blockchain networks.

Although this systematic review does not comprehensively analyze pre-2020 studies, these early theoretical frameworks and practical implementations are referenced to provide essential context and to guide readers who may wish to explore the foundational works that shaped the development of modern interoperability protocols [43].

In this SLR, only peer-reviewed papers, journal articles, and conference proceedings were included to ensure the credibility and academic rigor of the sources. Reviews and survey papers were excluded to focus on original research and empirical findings. Grey literature was deliberately excluded due to concerns regarding its typically low quality and the difficulty in drawing reliable conclusions prior to thorough [44]. This selection criterion ensures that the evidence synthesized in this review is grounded in validated and peer-reviewed research. The inclusion criteria will restrict studies to those published in English. There is evidence that the exclusion of articles written in languages other than English has only a minimal effect on the overall conclusions of the reviews [45].

3.5 Screening and Selection Process

The selection process was divided into three main phases: identification, screening, and inclusion. To minimize bias and enhance reliability, study selection was performed in duplicate by two independent reviewers (A.D. and T.F.A.). Disagreements were resolved through consensus discussion or consultation with the other reviewers (L.Y.P., C.S.K., and O.M.)

During the identification phase, search keywords were applied across all fields in the selected scholarly databases. The team documented the titles, datasets, abstracts, publication years, DOIs, and URLs in Google Sheets documents. In this phase, 9854 studies were initially identified, and a total of 677 studies were excluded for duplication.

The screening phase involves removing irrelevant studies. We identified these irrelevant studies by reading their titles and abstracts, indicating that they did not align with research objectives and questions. In total, 8836 were eliminated because of being irrelevant. In addition, 36 were removed as a result of accessibility restrictions.

All team members conducted a full-text review of the 305 papers to evaluate their suitability based on the predefined inclusion and exclusion criteria. Finally, in the inclusion phase, the shortlisted papers were reviewed collectively. Papers that failed to meet the criteria or were deemed irrelevant to the research questions. Finally, 56 studies were included in the final selection.

3.6 Quality Assessment

The quality of the included studies was critically appraised using the MMAT [19], a widely recognized instrument for evaluating research design, methodology, and potential biases. The MMAT checklist, consisting of five criteria, provides a systematic approach to assessing the reliability and significance of findings within their respective contexts. To minimize bias and enhance reliability, study selection and data extraction were performed independently by two reviewers, with disagreements resolved through consensus or consultation with a third reviewer.

3.7 Data Extraction

Data extraction is a crucial aspect of this review. The process involves identifying and extracting relevant data items to evaluate the quality of selected studies and to answer research questions. Table 4 provides a structured overview of the data categories extracted during the systematic review, including detailed descriptions of each item and the corresponding analytical approaches applied. It outlines the bibliographic and content-related data collected from the selected studies, specifying how each data type contributes to the descriptive, bibliometric, and content analyses performed in this review.

Table 4: List of data items

Data items	Data description	Analysis types
Bibliographic information.	The data about the title of the study, the year of publication, the name of the publication, as well as other relevant data, was obtained from academic databases.	Descriptive analysis and Bibliometric analysis.
The security analysis of the included study.	The data was obtained from the literature.	Descriptive analysis and Content analysis.

A team of four authors conducted the data extraction procedure, which was divided into two phases. In the initial phase, data was extracted from the included studies by two authors (A.D. and T.F.A.) using a predefined data extraction form in an independent manner. Any discrepancies were resolved through discussion. If disputes persisted, they were referred to two additional authors (L.Y.P. and C.S.K.) for arbitration.

A combination of manual and tool-assisted methods was implemented during the data extraction procedure. During the initial screening phase, Zotero, a reference management application, was employed to organize and manage the studies.

Microsoft Excel was utilized to store all extracted data and variables, which facilitated the systematic organization, categorizing, and filtering of the data for subsequent analyses. In instances where details were ambiguous or uncertain, assumptions were made in accordance with established standards in the literature. For instance, certain security properties were attributed to implicit features of protocols when they were frequently associated with those protocol categories.

3.8 Data Synthesis and Analysis

The goal of data synthesis is to assess and summarize the insights from the selected papers, presenting the results in a tabular format. This synthesized data serves as primary evidence to address the research questions, focusing on the security and privacy analysis guidelines for interoperability protocols across permissioned blockchains. This review incorporates various analytical approaches, including bibliometric analysis, descriptive analysis, and content analysis.

Bibliometric analysis is a methodological approach that integrates quantitative techniques—such as mathematical and graphical methods—to map the structure and evolution of research landscapes [46]. In this review, bibliometric analysis was used to provide a quantitative overview, including the distribution of studies by year and by publication name.

Content analysis is ideal for this SLR as it systematically identifies and interprets qualitative data—such as security properties, attacks, and countermeasures—from the 56 reviewed studies [47]. This method enables the authors to identify patterns, compare findings, and address the paper's research questions while highlighting gaps in interoperability research.

Microsoft Excel and Jeffrey's Amazing Statistics Program (JASP) were utilized to arrange extracted data and perform descriptive and statistical summaries. JASP is an open-source statistical software designed for both beginners and experts, featuring a user-friendly interface, automated statistical outputs, and advanced visualization capabilities, which made it particularly suitable for this systematic review [48,49]. Missing data was addressed by categorizing it as "Not Stated" in the table, and no data imputations or conversions were performed.

It is important to note that advanced statistical techniques, such as meta-analysis, are beyond the scope of this study. Instead, the review aims to deliver a structured and in-depth examination of security and privacy analysis guidelines for interoperability protocols across permissioned blockchains.

3.9 Motivation and Contribution

Blockchain technology has significantly transformed decentralized systems and enterprises by offering distributed, transparent, and tamper-resistant ledgers [1,2]. Its rapid adoption is evident: 76% of organizations have implemented blockchain, and 83% believe that digital assets will replace fiat currencies within the next decade [50]. Market projections further reinforce this trend. For instance, Grand View Research projects that the worldwide blockchain industry will attain USD 1431.54 billion by 2030 from 2023 to 2030. The blockchain industry is projected to expand from USD 2.89 billion to USD 137.29 billion between 2020 and 2027 [51]. These projections underscore robust confidence in the ongoing development and impact of blockchain technology.

Amid this expansion, enterprises are increasingly adopting permissioned blockchains tailored to specific sectors [40,41], such as the IoT [3–5], vehicular networks [6], and healthcare [7]. Despite their advantages—such as controlled access, higher transaction throughput, and regulatory alignment—permissioned blockchains have been criticized for reduced decentralization, scalability constraints, regulatory complexities, and potential data privacy concerns [40,41]. While frameworks such as Hyperledger Fabric [27,28], Quorum [30], Corda [31], and Multichain [32] have attempted to address these issues, several persistent challenges, notably interoperability, remain unresolved. In particular, the lack of seamless interaction between heterogeneous permissioned blockchains poses significant barriers to adoption. Interoperability protocols are designed to bridge these silos, enabling data exchange, asset transfers, and smart contract execution across otherwise isolated networks [9]. However, the security and privacy risks introduced by such protocols remain insufficiently understood.

The urgency of this issue is underscored by recent large-scale attacks on cross-chain bridges, which have led to losses exceeding USD 3.1 billion since 2021, with 65.8% of these losses originating from bridges relying on intermediary permissioned networks [52]. Cross-chain exploits now dominate the DeFi incident leaderboard [10], illustrating that interoperability mechanisms are a prime target for malicious actors. Although many of these attacks have occurred within public blockchains [53–56], permissioned blockchains face distinct challenges that are not adequately addressed by the existing body of research focused on public environments [15–17]. Unlike public blockchains, permissioned systems operate under strict authentication, privacy-preserving data-sharing requirements, and governance structures that demand tailored security frameworks.

This study focuses exclusively on permissioned blockchain interoperability to address this research gap. While references to public blockchain incidents are included to emphasize the severity and relevance of interoperability vulnerabilities, this review concentrates on permissioned ecosystems due to their unique trust assumptions and enterprise-driven requirements. By narrowing the scope in this way, we aim to develop insights that are directly applicable to high-assurance domains where confidentiality, regulatory compliance, and scalability are critical.

The main contributions of this paper are as follows:

- A structured overview of security and privacy properties critical to interoperability protocols.
- A comprehensive analysis of known attack types and the corresponding vulnerabilities they exploit.
- An overview of existing countermeasures, including their effectiveness and limitations.
- A synthesis of research gaps and future directions, identifying limitations in existing implementations and proposing areas for further investigation, including scalability, token standard handling, and real-world deployment.

4 Results

4.1 Study Selection

This section presents the results of the three stages of the PRISMA framework—identification, screening, and inclusion—as depicted in Fig. 3. The figure provides a detailed visualization of the study selection process, following the PRISMA 2020 guidelines. It outlines the number of records retrieved from the databases, the studies screened for relevance, those excluded based on eligibility criteria, and the final set of studies included for analysis.

The methodology strictly adheres to the PRISMA guidelines, including the use of a PRISMA flow diagram to detail the study selection process. A PRISMA checklist is provided as Supplementary Materials S1 File (S1 File: PRISMA 2020 checklist), ensuring transparency and reproducibility.

At the identification stage, we located a total of 9854 studies across all selected databases using the keywords specified in Section 3. The titles, databases, publication years, abstracts, and inclusion status of the considered studies are detailed in Supplementary Materials S4 File (S4 File: List of Included and Excluded Studies). Fig. 3 shows the distribution of studies identified in each database. After eliminating 677 duplicates, the remaining records were retained for screening.

During the screening stage, 8836 studies were excluded because their title, abstract, and keywords did not match the topic: blockchain and interoperability. Also, 36 studies were excluded due to inaccessibility.

This left 305 studies for full-text screening to evaluate their eligibility based on the established IC and EC. In this stage, 249 studies were excluded after full-text review. A comprehensive summary of the included and excluded studies is presented in Supplementary Materials S3 File (S3 File List of Excluded Studies).

Finally, in the inclusion stage, 56 studies that met all IC were selected for inclusion in this SLR.

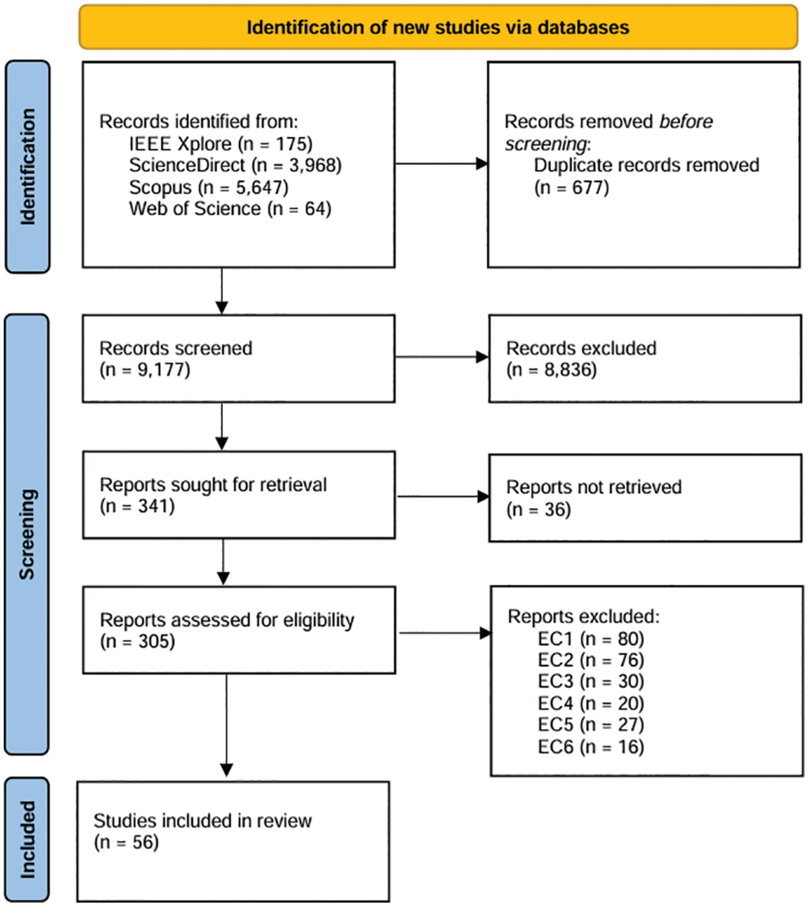


Figure 3: PRISMA flowchart for study selection

4.2 Quality of Included Studies

This section presents the methodological quality assessment of the included quantitative studies, evaluated using the MMAT. Of the 56 quantitative studies analyzed, 40 (71%) achieved MMAT scores of 100%, indicating high quality by fully meeting the assessment criteria. Eight studies (14%) scored 60%, reflecting medium quality with partial adherence to the criteria. The remaining eight studies (14%) were classified as low quality, primarily due to the absence of experimental implementations. A detailed quality assessment of the quantitative articles is provided in Supplementary Materials S2 file (S2 Table: Assessment of Study Quality–MMAT Tool).

4.3 Distribution of Papers by Year and by Publication Name

This section begins by examining annual publication trends related to interoperability protocols across permissioned blockchains. Fig. 4 illustrates the yearly distribution of studies published between 2020 and 2025. The number of studies increased steadily until peaking in 2022, followed by a decline and partial rebound. This surge in 2022 likely reflects growing interest in solving cross-chain communication challenges amid rapid blockchain adoption. The decline in 2023 may indicate a temporary shift toward practical implementation over theoretical research. The renewed activity in 2025 could suggest new challenges or innovations rekindling academic attention. Although 2025 shows a slight decline, it is important to note that the final search was conducted in May 2025, and thus the data may not capture the full publication output for that year. Despite this, interoperability protocols still represent a relatively modest portion of the broader computer science research landscape.

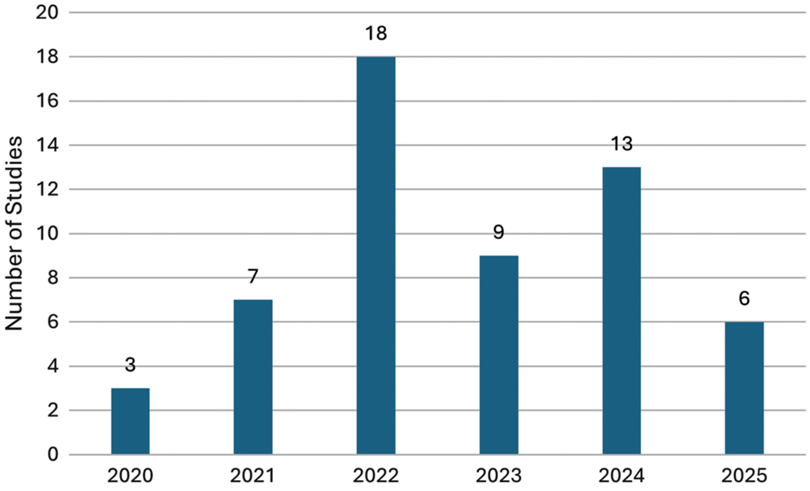


Figure 4: Annual distribution of studies on interoperability protocols in permissioned blockchains (2020–2025)

Fig. 5 illustrates the distribution of studies across academic conferences and journals included in this review of blockchain interoperability. The data reveals a strong focus on prominent IEEE and ACM conferences, such as the IEEE International Conference on Blockchain and ACM SIGSAC, as well as high-impact journals, including Future Generation Computer Systems and the IEEE Internet of Things Journal. Notably, the majority of sources contributed only a single article, underscoring the fragmented nature of research in permissioned blockchain interoperability. This distribution suggests that the field is still in an emerging phase, with research output dispersed across various venues rather than concentrated around established core platforms or thematic clusters.

4.4 Characteristic Studies

This section outlines the key characteristics of the reviewed interoperability protocols, categorized by their underlying mechanisms to facilitate cross-chain operations in permissioned blockchains. Table 5 summarizes the key characteristics of the studies included in the review, such as interoperability mechanisms (IM), the number of security and privacy properties (NSPP), the number of attacks (NA), implementation details (I), proof-of-concept evaluations (PoC), and publication types (Pub), including journal articles (J) and conference papers (C). The interoperability protocols examined in these studies are categorized into five mechanisms: sidechain, relay, notary scheme, HTLC, and hybrid mechanism.

Table 6 provides a statistical analysis of the interoperability mechanisms, implementation status, and publication types among the included studies. Among the included studies, 57% utilized the relay mechanism to facilitate cross-chain interoperability. Sidechain mechanism is employed in 14% of the studies, respectively. In contrast, only 6 studies (11%) adopt notary schemes, likely due to their high security risks. Meanwhile, hybrid mechanisms are implemented in just 4 studies.

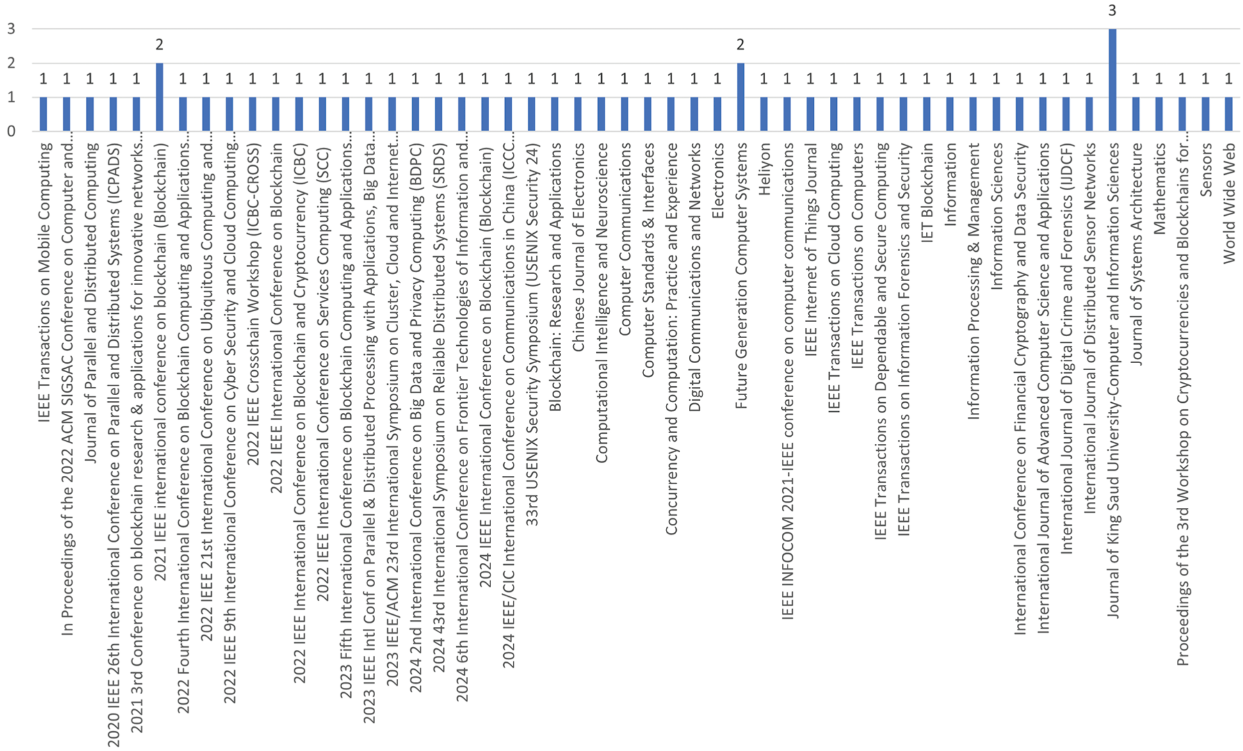


Figure 5: Frequency of studies by publication venue

Table 5: Study characteristics of the included studies

Ref.	IM	Participating blockchains	NSPP	NA	I	Pub
[57]	Sidechain	Ethereum, Hyperledger Fabric, and Burrow	4	4	PoC	C
[58]	Sidechain	Ethereum Private chains	5	0	No	J
[59]	Hybrid	Not stated	2	0	PoC	C
[60]	Notary scheme	Not stated	2	2	PoC	J
[61]	Relay	Hyperledger Fabric	5	1	Yes	C
[62]	Relay	PoW and PoS local chains	2	0	Yes	C
[63]	Relay	Not stated	3	0	Yes	C
[64]	Notary scheme	Polkadot substrate	3	0	Yes	C
[65]	HTLC	Bitcoin and Ethereum	1	2	Yes	C
[66]	Relay	Not stated	7	0	No	C
[67]	Relay	Bitcoin and Ethereum	1	2	Yes	C

(Continued)

Table 5 (continued)

Ref.	IM	Participating blockchains	NSPP	NA	I	Pub
[68]	Relay	Hyperledger Fabric	1	0	Yes	C
[69]	Relay	Hyperledger Fabric	1	1	Yes	C
[70]	Relay	Ethereum	2	2	Yes	C
[71]	HTLC	Not stated	1	1	PoC	C
[72]	HTLC	Not stated	3	1	No	C
[73]	Relay	Hyperledger Fabric	2	1	Yes	C
[74]	HTLC	Bitcoin, Ethereum, and Polygon	1	2	No	C
[75]	Sidechain	Not stated	1	6	No	J
[76]	Relay	Ethereum and hyperledger fabric	1	3	Yes	J
[77]	Relay	Hyperledger fabric	2	2	Yes	J
[78]	Sidechain	Monero and ZeroCash	1	1	Yes	J
[79]	Sidechain	Not stated	2	0	No	J
[80]	Relay	Not stated	1	0	No	J
[81]	Sidechain	Georli and Ganache	2	3	Yes	J
[82]	Relay	Polkadot	2	1	Yes	J
[83]	HTLC	Hyperledger fabric	1	0	Yes	J
[84]	Sidechain	Cosmos and Ethereum	0	2	Yes	J
[85]	Relay	Ethereum	1	2	Yes	J
[86]	Relay	Ethereum, Hyperledger fabric, and Bitcoin	1	0	PoC	J
[87]	Relay	Hyperledger Fabric, FISCO BCOS, and ChainMaker	1	0	Yes	J
[88]	Relay	Hyperledger Fabric and Ripple	1	0	Yes	C
[89]	HTLC	Ethereum, Hyperledger Fabric, and Bitcoin	1	1	Yes	J
[90]	Relay	Proof of Authority local chains	0	5	Yes	J
[91]	Notary scheme	Ethereum private chains	0	3	Yes	J
[92]	Relay	Hyperledger Fabric	0	1	No	J
[93]	Hybrid	Ethereum private chains and Hyperledger Fabric	0	2	Yes	J

(Continued)

Table 5 (continued)

Ref.	IM	Participating blockchains	NSPP	NA	I	Pub
[94]	Relay	Cosmos	0	1	Yes	J
[95]	Notary scheme	Ethereum private chains	0	2	Yes	C
[96]	Hybrid	Ethereum private chains	0	1	Yes	J
[97]	Relay	Hyperledger fabric	0	4	Yes	J
[98]	Notary scheme	Hyperledger fabric	1	1	Yes	J
[99]	Relay	Hyperledger fabric	2	3	Yes	J
[100]	Sidechain	Ethereum private chains and Hyperledger Fabric	2	0	Yes	J
[101]	Relay	Hyperledger fabric	2	0	PoC	J
[102]	Relay	Bitcoin, Ethereum, and FISCO BCOS	2	2	Yes	J
[103]	Relay	Hyperledger fabric	1	0	PoC	J
[104]	Relay	Hyperledger fabric and FISCO BCOS	1	2	Yes	J
[105]	Relay	Cosmos	1	2	Yes	C
[106]	Relay	Hyperledger fabric	1	0	Yes	C
[107]	Relay	Hyperledger fabric and FISCO BCOS	2	0	Yes	C
[108]	Relay	Cosmos	1	0	Yes	C
[109]	Relay	Not stated	1	0	Yes	C
[110]	Notary scheme	Ethereum, Hyperledger Fabric, and Cosmos	1	2	Yes	J
[111]	Relay	Hyperledger fabric	1	3	Yes	J
[112]	Hybrid	Proof of work chains	2	0	Yes	C

Note: IM: Interoperability Mechanism; NSPP: Number of security and privacy properties; NA: Number of attacks; I: Implementation; PoC: Proof of Concept; Pub: Publication types; J: Journal article; C: Conference.

Table 6: Statistical overview of interoperability mechanisms, implementation status, and publication types of the included studies

Category	Number of articles (n)	Average (n/56)
Interoperability mechanism		
Relay	32	57%
Sidechain	8	14%

(Continued)

Table 6 (continued)

Category	Number of articles (n)	Average (n/56)
HTLC	6	11%
Notary scheme	6	11%
Hybrid	4	7%
Implementation		
Yes	41	73%
No	8	14%
Proof of concept	7	13%
Publication types		
Journal article	32	57%
Conference	24	43%

Although 73% of the studies include an implementation of the proposed solution, a significant portion offer only a proof of concept (13%) or no implementation at all (14%). The included studies consist of 57% journal articles and 43% conference papers, indicating a balance between consolidating knowledge and emerging research. While journal publications suggest growing theoretical maturity, the substantial conference presence reflects ongoing innovation and experimentation in permissioned blockchain interoperability. The Ethereum blockchain and Hyperledger Fabric dominate the participating blockchain experiments in the included studies. Some studies have used Bitcoin to implement interoperability protocols due to its stability and simplicity. These implementations help validate protocol mechanisms that are applicable to permissioned settings.

Fig. 6 illustrates the comparative frequency of security and privacy properties addressed, as well as the attack vectors identified across the reviewed studies. The chart reveals that most interoperability protocols for permissioned blockchains document only a limited set of such concerns—despite over $3.1 billion in cross-chain attack losses since 2021 [10]. Notably, 93% of studies assessed fewer than four properties or attack vectors, reflecting a narrow research focus. This limited coverage indicates a fragmented understanding of the security landscape and suggests that critical vulnerabilities may be overlooked.

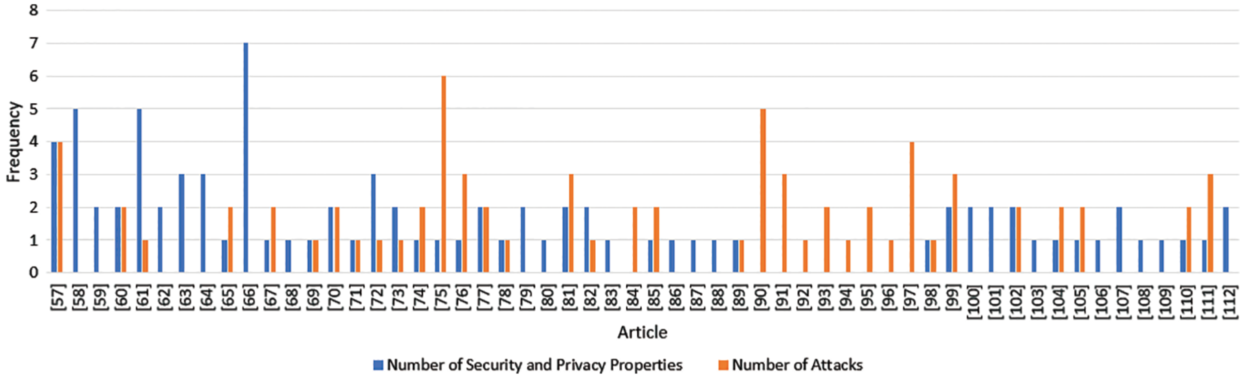


Figure 6: Comparative analysis of security and privacy properties vs. identified attacks in the reviewed studies [57–112]

4.5 Security and Privacy Properties

This section presents an analysis of the included studies that have an answer to Q1: What are the existing security and privacy properties of interoperability protocols across permissioned blockchains?

Interoperability protocols for permissioned blockchains are essential for facilitating seamless interactions across diverse blockchain networks. However, ensuring security and privacy within these protocols presents challenges due to varying levels of trust, control, and governance among permissioned blockchains. Key security and privacy properties—such as safety, liveness, and confidentiality—are critical for safeguarding cross-chain transactions and data within interconnected blockchains. This question provides an overview of these properties, which enhance reliable and privacy-preserving interoperability across permissioned blockchains.

Fig. 7 illustrates the distribution of how frequently each of the 18 identified security and privacy properties is addressed in the reviewed studies on interoperability protocols for permissioned blockchains. The distribution of security and privacy properties across the reviewed literature indicates a concentration of focus on a few key areas. Notably, atomicity, confidentiality, and integrity are the most frequently addressed properties. However, the analysis also uncovers underrepresented but essential properties. As an example, non-repudiation, crash fault tolerance (CFT), decentralization, and three ACID properties are significantly understudied despite their importance in a trustless, multiparty environment [8].

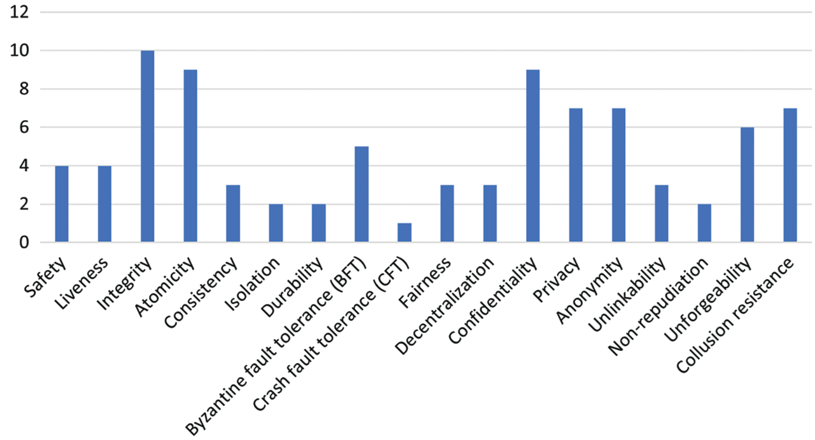


Figure 7: Frequency of security and privacy properties analyzed in the included studies

Table 7 presents a detailed mapping of key security and privacy properties to the interoperability mechanisms they address. The table also provides concise descriptions of each property, explaining how these properties contribute to ensuring the reliability, trustworthiness, and privacy of cross-chain operations.

Table 7: Mapping of security and privacy properties to interoperability mechanisms

Properties	Relay	Sidechain	HTLC	Notary Scheme	Hybrid	Description
Safety		[57,58]			[59]	It ensures that undesirable states are never reached [57].

(Continued)

Table 7 (continued)

Properties	Relay	Sidechain	HTLC	Notary Scheme	Hybrid	Description
Liveness		[57,58]		[60]	[59]	It guarantees that desirable states are successfully achieved [58].
Integrity	[62,63,66–69,104–106]			[64]		It ensures that cross-chain transactions remain consistent and untampered [67].
Atomicity	[61,66,70,108]	[58]	[71,72,83]		[112]	It ensures all transactions are either fully executed or not executed at all [61].
Consistency	[66,61]	[100]				It involves transitioning the blockchain from one valid state to another without breaking rules or causing manipulation [61].
Isolation	[61,66]					It ensures secure and independent execution of concurrent transactions [61].
Durability	[61,66]					It guarantees that changes resulting from a transaction are irreversible once executed [61].
Byzantine fault tolerance (BFT)	[70,80]	[57,58,79]				It enables blockchains to operate correctly and achieve consensus despite the presence of malicious or faulty nodes [80].

(Continued)

Table 7 (continued)

Properties	Relay	Sidechain	HTLC	Notary Scheme	Hybrid	Description
Crash fault tolerance (CFT)	[66]					It enables blockchains to operate correctly and achieve consensus despite the presence of system crashes [66].
Fairness	[82]	[78,81]				It ensures that all parties in a transaction receive their due rewards or losses are avoided [78].
Decentralization	[82]		[89]	[98]		It ensures that control is distributed among multiple entities, avoiding reliance on a central authority or trusted third party (TTP) [89].
Confidentiality	[61–63, 101,102]	[57,100]	[65]	[64]		It preserves privacy by preventing unauthorized access to data [61].
Privacy	[73,109,107,111]		[52,74]	[110]		It ensures that only authorized entities access and process sensitive information in compliance with user consent and regulations [73].
Anonymity	[76,77,99,107]	[58,75]		[64]		It protects the identities of entities by preventing external tracking of participants in cross-chain transactions [75].

(Continued)

Table 7 (continued)

Properties	Relay	Sidechain	HTLC	Notary Scheme	Hybrid	Description
Unlinkability	[99]	[78]			[112]	It prevents the correlation of multiple transactions or actions to the same entity, ensuring actions cannot be traced back to a single source [78].
Non-repudiation	[66]			[60]		It ensures that once a transaction or log entry is recorded, it cannot be denied or refuted by any involved party [60].
Unforgeability	[73,77,103]	[79,81]	[72]			It ensures that cryptographic proofs or signatures necessary for transactions cannot be falsified [72].
Collusion resistance	[63,85–88,101,102]					It prevents entities from collaborating to manipulate cross-chain transactions or consensus processes [85].

Table 8 summarizes the number and percentage of Security and Privacy Properties associated with each interoperability mechanism. Relay-based protocols demonstrate the most comprehensive coverage, addressing 89% of the identified properties. In contrast, sidechain mechanisms cover 56%, while HTLC and notary-based approaches exhibit substantially more limited coverage, indicating potential security blind spots in these mechanisms.

Table 8: Distribution of security and privacy properties by interoperability mechanism

Interoperability mechanism	Number of properties (n)	Average (n/18)
Relay	16	89%
Sidechain	10	56%
HTLC	5	28%
Notary scheme	7	39%
Hybrid	4	22%

In conclusion, the findings reveal a fragmented and uneven landscape in cross-chain security research, with many properties rarely examined, highlighting the urgent need for more comprehensive and balanced security assessments across all protocol types. Relay-based protocols demonstrated the broadest coverage, while HTLC and notary-based mechanisms were more limited. Important features such as non-repudiation, CFT, decentralization, and the three ACID properties are not studied enough, even though they are crucial in a system where trust is not guaranteed among multiple parties.

4.6 Attack Types

This section presents an analysis of the included studies that have an answer to Q2: What are the specific attacks associated with interoperability protocols in these environments?

Blockchain interoperability has become essential as permissioned blockchain networks increasingly interact to enable data sharing, asset exchange, and collaborative processes across organizational boundaries. However, the growth of interoperability protocols has also introduced various security vulnerabilities, which adversaries exploit to compromise data integrity and confidentiality. Understanding these attacks is crucial to developing more resilient interoperability protocols. This section provides an overview of these attacks.

Fig. 8 illustrates the distribution of the 31 distinct attack types identified across the reviewed studies on interoperability protocols for permissioned blockchains.

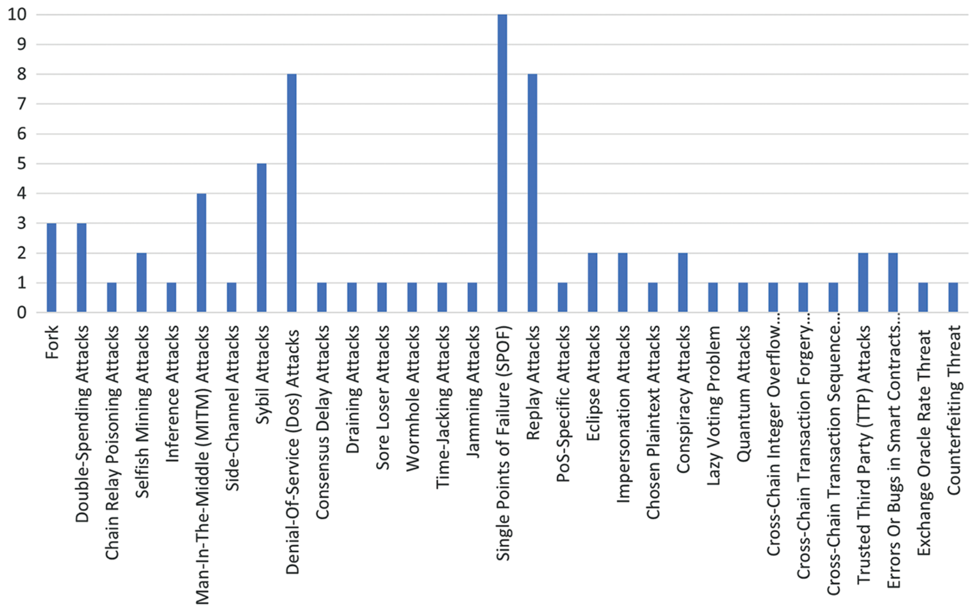


Figure 8: Frequency of attack types analyzed in the included studies

Fig. 8 illustrates that over 58% of the identified attack types were addressed in only a single study, indicating a highly fragmented and narrowly focused threat analysis in the current literature. Although attacks such as Single Point of Failure (SPOF), DoS, and Replay attacks have received comparatively more attention, a substantial number of known threats remain largely unexamined. This lack of comprehensive coverage highlights a critical gap in the field and underscores the urgent need for more systematic, wide-range security evaluations in the context of cross-chain interoperability.

Table 9 presents a detailed mapping of various attack types to the interoperability mechanisms they target. The table also includes concise descriptions of each attack, outlining how these vulnerabilities exploit weaknesses in blockchain consensus, transaction validation, or cross-chain communication.

Table 9: Mapping of attack types to interoperability mechanisms

Attack types	Relay	Sidechain	HTLC	Notary scheme	Hybrid	Description
Fork	[70,90]	[57]				When competing blocks are mined simultaneously, leading to orphaned blocks and temporary inconsistencies in the blockchain [90].
Double-spending attacks	[77]		[74]	[60]		Deceiving two separate entities into believing they have both been paid with the same coins. If successful, only one transaction is confirmed by the blockchains, while the attacker obtains both products from the two entities [74].
Chain relay poisoning attacks		[75]				Corrupting the trusted relay system by triggering a blockchain reorganization, invalidating previously accepted transactions. This attack exploits the probabilistic finality of the source blockchain and may lead to incorrect verification of cross-chain transactions [75].
Selfish mining attacks	[90]		[74]			In PoW blockchains, malicious miners withhold valid blocks until they can mine two sequential blocks, doubling their rewards. In PoS blockchains, selfish behavior incentivizes validators to create separate forks faster than the network can produce blocks [74].
Inference attacks		[75]				When intermediaries deduce sensitive transaction information, such as the total value of transferred assets, by analyzing partial amounts in cross-chain transfers. They may also infer the source of funds, compromising user anonymity [58].
Man-in-the-middle (MITM) attacks	[61,76,99]		[65]			Intercepting and altering real-time communication between entities without their knowledge [76].
Side-channel attacks		[78]				Exploiting timing anomalies during cross-chain transactions. Adversaries can infer a receiver's identity by observing delayed responses caused by locked wallets [78].
Sybil attacks	[111]	[57]		[60,91,110]		Creating multiple fake identities to gain disproportionate control or influence over the network [60].
Denial-of-service (Dos) attacks	[67,76,90,92,104,111]	[57]		[110]		Flooding the network with spurious messages or by withholding responses during multi-signature collection, causing failures in cross-chain transactions [57,67].
Consensus delay attacks	[90]					Sending false blocks to hinder or prevent consensus among network participants [90].

(Continued)

Table 9 (continued)

Attack types	Relay	Sidechain	HTLC	Notary scheme	Hybrid	Description
Draining attacks			[65]			Exploiting vulnerabilities in cross-chain transactions to siphon assets. For example, in HTLCs, a malicious responder may withhold exchanges, retaining control of locked assets [65].
Sore loser attacks					[93]	Disrupting a partially executed cross-chain transaction if the outcome is unfavorable [93].
Wormhole attacks					[93]	Involving collusion between two nodes to bypass intermediaries, enabling them to unlock assets and steal transaction fees [93].
Time-jacking attacks	[90]					Exploiting incorrect timestamps on blocks, causing target nodes to reject valid blocks [90].
Jamming attacks	[94]					Overwhelming light clients with numerous headers to verify, which increases transaction failure rates [94].
Single points of failure (SPOF)	[82,85]	[81,84]	[72,89]	[91,95,98]	[96]	Trusted third parties (TTPs) or Oracles fail, disrupting cross-chain transactions [81,91].
Replay attacks	[70,76,97,67,99, 102,104]	[75]				Replicating legitimate sidechain transactions on the mainchain or repeatedly broadcasting verified blocks to mislead the network [76].
PoS-specific attacks	[85]					Nothing-at-stake and long-range attacks exploit PoS vulnerabilities, such as validators signing multiple chains or using compromised keys to create alternative chains [85].
Eclipse attacks	[111]	[75]				Isolating a target node by monopolizing its connections, distorting its perception of the network, or blocking legitimate updates [75].
Impersonation attacks	[99]	[57]				In consortium blockchains, attackers impersonate spokespeople to disseminate false information [57].
Chosen plaintext attacks	[69]					Exploiting encryption schemes by requesting arbitrary plaintexts to analyze the resulting ciphertexts and gather information about the encryption key [69].
Conspiracy attacks	[77]			[95]		When group members collaborate to disclose secret keys [95].
Lazy voting problem				[91]		Oracle nodes submit incorrect or identical responses to save computational resources, undermining consensus integrity [91].
Quantum attacks			[71]			Quantum computers exploit algorithms like Shor's and Grover's to break cryptographic keys and hash functions, compromising blockchain security [71].
Cross-chain integer overflow attacks	[97]					Manipulating transaction amounts to exceed system limits, altering account states improperly [97].
Cross-chain transaction forgery attacks	[97]					Exploiting user smart contracts to forge transactions [97].
Cross-chain transaction sequence attacks	[97]					Reordering transactions due to network delays, causing inconsistencies [97].

(Continued)

Table 9 (continued)

Attack types	Relay	Sidechain	HTLC	Notary scheme	Hybrid	Description
Trusted third party (TTP) attacks		[81,84]				Exploiting reliance on intermediaries, manipulating cross-chain transactions, or disclosing private information [84].
Errors or bugs in smart contracts threat	[102]	[81]				Errors in smart contracts can hinder successful cross-chain transactions [81].
Exchange oracle rate threat		[75]				Manipulating exchange rates undermines collateralization, threatening security [75].
Counterfeiting threat		[75]				Issuing tokens without equivalent collateral backing introduces critical risks [75].

Table 10 summarizes the number and percentage of attacks associated with each interoperability mechanism. The data show that relay (65%) and sidechain (45%) mechanisms are the most frequently analyzed in terms of attack vectors, suggesting a concentrated research focus on these approaches. In contrast, HTLC-based mechanisms (19%), notary schemes (19%), and hybrid models (10%) exhibit significantly lower coverage. This disparity points to notable research blind spots, implying that key attack surfaces in these less studied mechanisms may be insufficiently understood or documented. Such gaps underscore the need for broader and more balanced security analyses across all interoperability designs to ensure comprehensive threat mitigation.

Table 10: Distribution of identified attacks by interoperability mechanism

Category	Number of attacks (n)	Average (n/31)
Relay	20	65%
Sidechain	14	45%
HTLC	6	19%
Notary scheme	6	19%
Hybrid	3	10%

In conclusion, the findings reveal a fragmented and uneven landscape in cross-chain security research—where most attack types are rarely studied, and certain interoperability mechanisms like HTLC, notary schemes, and hybrids remain under-analyzed—highlighting the urgent need for more comprehensive and balanced security assessments across all protocol types.

4.7 Countermeasures

This section presents an analysis of the included studies that have an answer to RQ3: What countermeasures have been proposed to preserve the security and privacy of such protocols?

Researchers have proposed a range of countermeasures to maintain the security and privacy of interoperability protocols. These countermeasures address critical security and privacy properties such as safety, integrity, confidentiality, and resistance to specific attacks, including double-spending and Sybil attacks. The following sections describe how each study achieves secure and private properties and resists attacks on interoperability protocols.

4.7.1 Countermeasures to Maintain Security and Privacy Properties

Ensuring robust security and privacy is essential for the dependable operation of interoperability protocols in permissioned blockchain systems. Numerous studies have proposed countermeasures that reinforce key system properties such as safety, liveness, integrity, and confidentiality. This section categorizes and summarizes these countermeasures based on the specific security and privacy attributes they aim to preserve.

- Safety and liveness: Safety and liveness have been maintained through various approaches proposed in the literature [57,59,60]. For instance, in [57], safety and liveness are provided by a two-step consensus mechanism: transactions are first endorsed on the permissionless blockchain and only committed to the permissioned chain once more than two-thirds of the permissioned entities have voted in favor, guaranteeing safety. Liveness relies on the underlying permissionless blockchain interface. Similarly, the approach in [59] uses a threshold signature scheme to assure both safety and liveness. Finally, CrossLedger [60] focuses on timeliness: it achieves liveness by enforcing that all necessary verifications be completed within a specified deadline, preventing indefinite delays.
- Integrity and Confidentiality: Integrity and confidentiality have been preserved through various cryptographic and architectural mechanisms proposed in the literature [57,62–65,67–69,100–102,104–106]. Several works reinforce integrity and tamper-evidence by combining cryptographic hashes with consensus. Study [67] uses a smart-contract consensus mechanism to strictly enforce transaction rules, preserving integrity across chains. Similarly, study [62] integrates standard hashing algorithms into a consensus mechanism. Traditional encryption schemes also play a major role. In [105], data is encrypted block-wise using secp256k1 elliptic-curve keys combined with 3DES, and only decrypted upon receipt. Also, transactions are encrypted using an encryption scheme such as Rivest-Shamir-Adleman (RSA) to achieve confidentiality [57,62,63,101]. Time-release encryption (TRE) in [65] further guarantees that sensitive payloads remain unreadable until explicit conditions—such as block height or timestamps—are met. BeDCV [69] adopts a modified Paillier homomorphic scheme so that the supervision chain can verify computations on encrypted data without ever seeing plaintext, while bilinear pairings validate the completeness of aggregated audit data. DataFly [100] utilizes integrated signature and encryption (ISE) and ECDSA-based key extraction. To prevent insider threats, study [64] and IvyCross [102] both implement critical key operations within a Trusted Execution Environment (TEE) like Intel SGX. Even a malicious committee member cannot extract key material, thus safeguarding both integrity and confidentiality. Protocols such as [104] store Merkle-root commitments on the origin chain and use smart contracts for verification, while Refs. [68] and [63] rely on the unforgeability of digital-signature schemes and the discrete logarithm (DL) hardness to achieve end-to-end integrity. Finally, in [106], the method uses certificate-based authentication to ensure secure communication.
- Atomicity, Consistency, Isolation, and Durability: The ACID properties—Atomicity, Consistency, Isolation, and Durability—have been addressed in the following studies [58,61,66,70,72,100,108]. To ensure atomicity, many protocols implement coordination contracts that document all possible cross-chain states, and a two-phase commit (2PC) or announcement-rollback mechanism ensures that either every participant agrees to commit or all changes are rolled back on timeout. In both [58] and [70], each node starts a local timer when a transaction begins; if it expires, the protocol triggers a rollback. Avalon [108] achieves atomicity through layered state caching, optimistic concurrency control, and a state synchronization protocol that coordinates commit decisions across blockchains, while ODAP-2PC in Hermes [66] uses a write-ahead log and self-healing recovery to guarantee that each transaction either fully commits or aborts. Cross-chain consistency follows strict ordering and quorum-based commit rules. Coordination contracts in [58] and [72] enumerate valid state transitions, ensuring every

participant sees the same history. DataFly [100] adds a Peg consensus mechanism to authenticate and finalize data transfers across permissioned chains, with formal proof that an honest majority preserves consistency. The protocol in [61] maintains isolation by routing messages through dedicated channels so that only authorized groups can observe or influence a transaction's intermediate state. To maintain durability, once ordering entities agree, new blocks containing cross-chain transactions are generated and propagated throughout the network. As shown in [61], durability is guaranteed by anchoring each committed transaction to the immutable blockchain ledger, making it resilient to subsequent failures or rollbacks.

- BFT and CFT: BFT and CFT have been addressed in several studies as essential properties for ensuring reliability in cross-chain operations [66,88]. To increase the BFT threshold, Ref. [80] proposes a weighted PBFT cross-chain consensus that groups nodes by security level and assigns high voting weights to more trusted participants, enabling the system to tolerate up to n/2 weighted faults. Hermes [66] achieves crash resilience via a blockchain-backed log storage API: every step of a cross-chain transaction is immutably recorded so that, in the event of a gateway or system crash, the transaction can be resumed or rolled back without violating consistency.
- Fairness: Fairness is ensured in [81] by providing validators with equal opportunities to participate, along with clearly defined rewards and penalties to incentivize honest behavior and discourage misconduct.
- Non-repudiation: Non-repudiation is maintained by gateways that ensure log entries remain unaltered and that the protocol reaches completion, thereby preserving the undeniability of recorded transactions [66].
- Unforgeability: Unforgeability has been addressed in several studies [72,73,77,79,103]. For instance, in [77], group signatures are protected by requiring each node to present its enrollment certificate to a group manager, who then issues a one-time transaction certificate. Papers [73,103] rely on well-studied cryptographic assumptions: resisting hash collisions and the DL problem make forging proofs computationally infeasible, while the Advanced Gamma Multi-Signature (AGMS) in EDCA is provably secure under the DL assumption. Ref. [79] embeds non-interactive proof-of-proof-of-works (NIPoPoWs) proofs under the assumption of an honest majority: during a contestation period, honest nodes can publish counter-proofs to detect any adversarial chain attempt. Finally, Ref. [72] shows that under their stateless SPV model, the cost of forging a valid proof exceeds any possible financial gain, making forgery economically irrational.
- Collusion resistance: Collusion resistance has been addressed in several studies [63,85–88,101,102]. A modified PBFT in [86] assigns higher voting weights to smaller, well-trusted node groups, making bribery or cartel formation both more costly and operationally cumbersome. Verilay [85] leverages PoS's finality: because blocks cannot be reverted without controlling a majority of stake, validator collusion to rewrite history becomes economically infeasible. XChange [88] restricts how many cross-chain trades a single participant may open and employs TrustChain's immutable logging to automatically flag and penalize suspicious patterns. ChainKeeper [87] uses a verifiable node random selection (VNRS) along with verifiable identity threshold signatures (VITS) so that forging a collaborative signature without the required threshold is impossible, even if both business and supervision nodes collude. The randomized audit sampling in [63] allows the system to catch collusion with high probability, while IvyCross [102] and GAM [101] introduce incentive models and distributed re-encryption links, respectively, to ensure that no single dishonest node gains enough information or reward to justify a collusion attack.
- Decentralization: Decentralization has been addressed in studies [89,98]. AucSwap in [89] avoids centralized control by leveraging a decentralized Vickrey auction mechanism combined with the atomic swap mechanism. The HMNGCCM framework [98] enhances decentralization through a combination of hierarchical notary management, functional division, dynamic reputation evaluation, and robust

protocol design. By classifying notaries at junior, intermediate, and senior levels based on reputation and requiring deposits and verification, it discourages malicious participation and reduces centralization. The clear separation of transaction execution further strengthens decentralization.

- Privacy-preserving properties: Privacy-preserving properties have been implemented in several studies [58,64,72–76,99,107,109,111,112]. In [73], privacy is ensured as long as the DL problem remains computationally hard within the multi-signcryption algorithm. Study [74] integrates DMix with a threshold-signature protocol to increase the difficulty of determining the number of participants in cross-chain transactions. Likewise, Study [58] uses Boneh–Lynn–Shacham (BLS) threshold signatures—an external party can verify validity without learning individual signer identities. BxTB [72] reduces personal data leakage by relying on stateless SPVs, while ring-signature and Ring-VRF constructions in [64,76] ensure that any group member may have signed a message, but it's cryptographically infeasible to pinpoint who. ZCLAIM [75] leverages Zero-Knowledge Succinct Non-interactive ARgument of Knowledges (ZK-SNARKs) to hide both transaction amounts and participant identities in a succinct non-interactive proof, and zkCross [112] further obscures receiver addresses through denomination-based mixing. Identity chains in [107] register Decentralized identifiers (DIDs) tied to verifiable certificates, using the DID hash as a non-linkable watermark for transaction verification, while study [111] combines DID authentication with Zero-knowledge proofs for private mutual node authentication. In [99], the system maintains anonymity and unlinkability under the Dolev–Yao threat model. For enterprise data, study [109] applies threshold homomorphic encryption and proxy re-encryption so that only authorized parties holding partial decryption keys can access sensitive credit information, and offline verification stops unauthorized replay.

4.7.2 Countermeasures to Prevent Attacks

Mitigating security threats is a critical aspect of designing resilient interoperability protocols for permissioned blockchains. A wide range of studies have proposed defense mechanisms targeting specific attack vectors that exploit vulnerabilities in cross-chain communication. This section organizes and synthesizes these countermeasures according to the type of attack they address, highlighting the strategies employed to detect, prevent, or neutralize such threats across various interoperability models.

- Fork: Forks can delay transaction finality and open up reorg attacks. Polkadot [70] mitigates this with the GRANDPA finality gadget (a GHOST-based recursive ancestor prefix protocol), while Ref. [90] proposes monitoring block-propagation delays and average network hash rate as real-time fork detectors.
- Double-spending attacks: Double-spending attacks are prevented when ensuring that an asset isn't spent twice across chains requires undeniable proof of state. The relay-chain design in [77] stores only block headers to validate balances, study [74] relies on a configurable confirmation depth and precise finality timing, and Ref. [60] adds a dual-verification step: trust is established among asset-forwarders on both chains, then traceable ring signatures confirm each cross-chain transfer.
- Chain relay poisoning attacks: Chain relay poisoning attacks are defended by requiring a minimum block depth for finality before accepting cross-chain data, though it warns that eclipse attacks on isolated relayers can still lead to poisoning [75].
- Selfish mining attacks: Selfish mining attacks are addressed in studies [74,90]. The protocol in [74] again uses confirmation counts and timing constraints to limit selfish-mining impact, and study [90] suggests tracking the average network hash rate among nodes, the total hash rate of the target blockchain, and the delay in block propagation to flag anomalous withholding behavior.

- Inference attacks: Inference attacks are prevented in ZCLAIM [75] by splitting transfers into randomized sub-amounts routed through multiple intermediaries, so no single relay sees the full value—thereby thwarting end-to-end inference.
- Sybil attacks: Sybil attacks are prevented by leveraging permissionless blockchains as an interface [57], inheriting their native Sybil defenses—consensus makes it computationally or economically infeasible to spin up many fake nodes. Study [91] requires nodes to lock up a stake and biases rewards toward larger deposits, disincentivizing stake fragmentation across multiple identities. Cross-Ledger [60] first verifies asset ownership and then applies an asset-forwarder-selection algorithm plus traceable ring signatures to ensure that only legitimate forwarders can act—any forged or duplicate identity would lack the necessary signed proofs. Similarly, study [77] authenticates every node before it joins the cross-chain transfer, preventing one actor from registering multiples. XPull [111] prevents unauthorized connections by requiring all participants to furnish zero-knowledge proofs linked to on-chain public keys, and the hybrid scheme in [110] layers homomorphic encryption (P-ElGamal), threshold signatures, and secure MPC (SMPTC3) so that each operation is cryptographically tied to a unique, non-replicable identity.
- DoS attacks: DoS attacks are mitigated by blocking spam and malicious requests at the source. For example, study [76] introduces a DoS-resistant contract wrapper that logs request rates, filters low-gas calls, and blacklists offending addresses. Bridgechain [104] avoids single-point overload by sharding validation across multiple nodes, and study [57] aggregates BLS signatures into a transparent multisig—any node that withholds its share is quickly detected and excluded. ARC [92] secures inter-node communication with Transport Layer Security (TLS) and Secure Socket Layer (SSL) protocols and embeds flow monitoring in the relay chain to catch anomalous traffic from compromised insiders. XPull [111] further prevents DoS by periodically reassigning communicator groups and marking unresponsive parachains as faulty. In [67], Charging per-transaction fees makes large-scale flooding uneconomical, while the hybrid P-ElGamal plus threshold-MPC scheme in [110] ensures only stake-backed identities can submit high-volume requests.
- Replay attacks: Replay attacks are prevented by ensuring that cross-chain transactions cannot be executed more than once. Most protocols [67,70,75,76,97,99,104] tag each cross-chain request with a fresh, randomly generated nonce; the contract checks and consumes this nonce on execution, making any replay immediately invalid. IvyCross [102] goes further by requiring on-chain proof of progress and a lightweight challenge–response: if a participant attempts to replay a transaction without new evidence, the system triggers a rollback, preserving both safety and liveness.
- SPOF: SPOF is prevented by employing smart contracts [72,85,96] and a notary group [95,98] instead of a single notary helps reduce centralization and SPOF.
- PoS attacks: PoS-related attacks are mitigated in Verilay [85]. The protocol addresses potential security risks of the nothing-at-stake attack by ensuring that only finalized blocks are used, which have been agreed upon by a majority of validators. Finalized blocks are considered irreversible, which minimizes the risk of double-spending and other fork-based attacks. Verilay's reliance on finalized blocks also helps mitigate long-range attacks, where attackers might try to rewrite a blockchain's history if old keys are compromised.
- TTP attacks: TTP attacks are mitigated in several studies [81,84]. ZkBridge [84] eliminates the need for a TTP by embedding ZK-SNARK proofs into every cross-chain transaction, allowing on-chain validation without external oracles. In [81], validators and TTPs are required to deposit collateral, which is forfeited in cases of malicious conduct. Moreover, validator groups have the authority to temporarily disable or enable TTPs, preventing their operation. Moreover, the article proposes utilizing decentralized Oracle networks instead of TTP to employ independent entities for verification.

- Conspiracy attacks: Conspiracy attacks are addressed in studies [87,95]. The system in [95] demands validating transactions from a larger proportion of the notary's group, making it considerably more challenging for a small group of notaries to manipulate results. In ChainKeeper [87], a refined threshold signature scheme known as the VITS is introduced, which effectively verifies the identity of the signer and provides resistance to conspiracy attacks commonly associated with threshold signature schemes.
- Lazy voting problem: The lazy voting problem is addressed in [91] by requiring nodes to supply specific information—such as the block number in which a transaction is included—as part of their participation. By enforcing meaningful data contribution and validation, the system ensures active engagement from nodes, thereby preventing passive or non-contributory voting behavior.
- Sore loser and wormhole attacks: Sore loser attacks are mitigated by preventing participants from abandoning a transaction once it has been initiated. The protocol in [93] enforces strict withdrawal rules and liquidated damages—anyone who fails to complete the handoff forfeits their bond, which is redistributed to honest parties. The same liquidated damages framework also deters covert wormhole attacks: if an attacker tries to shortcut the protocol, they lose their stake and face financial penalties. A designated notary group handles token unlocking, and time-locked exchange of the preimage ensures that both sides either complete the swap simultaneously or neither receives funds, preventing any asset theft.
- Cross-chain integer overflow attack: Cross-chain integer overflow attacks are prevented in [97] by adding checks on transaction amounts and implementing safe arithmetic functions, such as Ethereum's SafeMath, to avoid overflow errors.
- Cross-chain transaction forgery attack: Cross-chain transaction forgery attacks are prevented in [97] by designing secure chaincodes with verification mechanisms, such as public and private keys, to prevent unauthorized interactions and the adding of false transactions.
- Cross-chain transaction sequence attacks: Cross-chain transaction sequence attacks are prevented in [97] by adding flags to confirm transactions' order.
- Exchange Oracle rate threat: In [75], the protocol suggests using decentralized Oracles and multiple data sources to attain reliability and avoid the exchange Oracle rate threat.
- Counterfeiting threat: In [75], intermediaries are required to periodically provide proof of their balance to prove that issued tokens are properly collateralized by corresponding assets on the source chain.
- MITM attacks: HT2REP [65] adopts a hierarchical blockchain data structure and performs Elliptic Curve Diffie–Hellman key negotiation on-chain so that only the intended parties can derive the session keys. In [76], ring signatures conceal the origin of a transaction among a set of possible signers, making it infeasible for a MITM attack to alter or forge messages undetected. A Zero-knowledge proof-based handshake in [61] lets two chains mutually verify each other's identities without revealing secret keys. Finally, in [99], standard encryption plus authenticated key exchange ensures confidentiality and integrity of cross-chain payloads, thwarting any MITM that lacks the negotiated keys.
- Draining attacks: In [65], the initiator's American option advantage and the responder's potential for launching a draining attack are mitigated through the use of scalable smart contracts, TRE locks (TREL), and hash time locks (HTL).
- Eclipse attacks: Eclipse attacks are prevented in XPull [111] by ensuring that a single honest communicator or storer suffices to sustain communication. In cases of disruption, XPull employs randomized reconfiguration to replace isolated nodes and restore state transfer.
- Impersonation attacks: The proposed work in [57] employs cryptographic techniques, including digital signatures, to authenticate all communications. In [99], Impersonation attacks are prevented through robust zero-knowledge proof-based identity authentication.

- Chosen plaintext attacks: In [69], the analysis highlights that the modified Paillier encryption provides semantic security under the Decisional Composite Residuosity Assumption (DCRA), which is critical for protecting against chosen plaintext attacks.
- Quantum attacks: The paper proposed in [71] a lattice-based digital signature scheme, known for its quantum security, making it a viable alternative to protect blockchain systems from future quantum-based threats.
- Side-channel attacks: The protocol [78] uses a zero-knowledge proof protocol to break the linkability of cross-chain transactions and prevent attackers from correlating across-chain actions.
- Consensus delay attacks: The article [90] identifies three indicators to detect consensus delay attacks: the delay time in block propagation, the average spending time of the transaction, and the average spending time of each transaction.
- Time-jacking attacks: In [90], the authors identified two indicators to detect a time-jacking attack: the delay in block propagation and transaction ordering. These indicators are used to effectively evaluate the validity of the process and transmission timing.
- Jamming attacks: Jamming attacks are prevented in [94] by enhancing the capability of blockchains to confirm the authenticity and intent of transactions more robustly, potentially by analyzing the frequency and pattern of transactions coming from certain nodes. Another strategy is to make cross-chain requests atomic, ensuring that a request isn't processed unless all its components are verified and executed simultaneously, reducing the chance of manipulation.
- Smart contract bugs: Smart contracts are subject to audits using tools like Mythril and tests utilizing the Truffle framework to detect and correct possible errors or bugs [81]. In IvyCross [102] ensures correct contract execution in concurrent environments using optimized TicToc-based concurrency control that checks data consistency with timestamps.

4.8 Analysis of Heterogeneity among Studies

The synthesis revealed notable heterogeneity across studies driven by differences in protocol maturity and research focus, leading to inconsistencies in reported security and privacy analyses. The overrepresentation of relay-based protocols alongside the underreporting of negative results indicates the presence of topic and publication bias. These variations highlight the need for standardized evaluation criteria and more inclusive literature sampling in future reviews.

4.9 Risk of Reporting Bias

While this review applied rigorous IC and searched multiple databases, there is a moderate risk of reporting bias across the synthesized literature. Most included studies are peer-reviewed academic publications, with minimal inclusion of industry-led evaluations. This may lead to the underrepresentation of unsuccessful implementations, unpublished vulnerabilities, or commercially sensitive failures—particularly in areas such as privacy, validator incentives, and cross-chain contract security. Future reviews may benefit from incorporating more diverse publication types, such as white papers and industry reports.

5 Discussion

This discussion synthesizes key findings from the review and is structured into two main parts. The first subsection, Identifying Gaps, highlights unresolved research challenges and limitations in current studies on permissioned blockchain interoperability. The second subsection, Future Research Directions, outlines forward-looking priorities and emerging opportunities to guide future advancements in secure and scalable cross-chain protocols.

5.1 Identified Gaps

This review systematically investigates the security analysis landscape of blockchain interoperability, with a particular focus on permissioned blockchain systems. It presents the current approaches to evaluating the security of cross-chain protocols and synthesizes key findings from the literature. Importantly, it highlights several security gaps and unresolved challenges that were identified during the review process. These identified gaps fall strictly within the defined scope of our research and underscore critical areas requiring further investigation.

While the annual growth in publications reflects increasing academic interest in secure cross-chain systems, the overall number of studies remains modest compared to substantial economic investments in blockchain technologies—particularly as blockchain adoption accelerates across decentralized ecosystems, enterprise applications, and DApps.

Although this review captures a wide spectrum of attacks and defenses, it is not without limitations. The selection of literature was restricted to studies published between 2020 and 2025 and conducted primarily in English, which may exclude earlier foundational work or emerging research in other languages. Additionally, the inclusion criteria, while rigorous, may have introduced bias by favoring technical studies over industry-led white papers. Future research should broaden the scope by incorporating gray literature and unpublished evaluations of deployed systems to create a more holistic evidence base.

Another methodological limitation is that we did not register our review protocol in a public database. Although we adhered to PRISMA guidelines throughout our process, preregistering the protocol would have improved transparency and reproducibility. Registration helps to avoid redundant efforts, minimize reporting bias, and enable peer evaluation of the methodology before data collection. Future reviews in this area should consider protocol registration to reinforce rigor and openness.

5.1.1 Limited Security and Privacy Coverage

Notably, 93% of the reviewed studies assessed fewer than four security properties or attack vectors, revealing a significant gap in the literature. This narrow scope reflects a fragmented and incomplete understanding of the security landscape in blockchain interoperability. The limited analytical coverage raises concerns that key vulnerabilities may be systematically overlooked, highlighting an urgent need for more holistic and in-depth security evaluations in future research.

This review finds a clear disparity in the depth and breadth of security analysis across different interoperability mechanisms. While relay-based protocols show relatively robust coverage, the limited attention given to security and privacy properties and attack vectors in HTLC- and notary-based systems suggests that these mechanisms may lack sufficient scrutiny in the literature. This uneven distribution of analyses points to a critical gap in current research, where certain widely adopted interoperability solutions remain underexamined from a security standpoint. Addressing this gap is essential to ensuring that all mechanisms are subjected to rigorous and uniform security evaluations, thereby reducing the risk of unanticipated vulnerabilities in real-world deployments.

5.1.2 Underexplored ACID Properties and Decentralization

ACID properties and decentralization are foundational to secure and reliable interoperability protocols [8]. ACID ensures that cross-chain transactions are executed consistently, irreversibly, and with preserved data integrity, while decentralization upholds the core principles of blockchain systems.

Despite their recognized importance, both are underrepresented in current research. This gap is partly due to the technical complexity of enforcing ACID properties across heterogeneous blockchains with differing architectures, consensus mechanisms, and data formats [8,21]. Isolation requires independent execution of cross-chain transactions, yet variations in consensus and transaction ordering hinder this guarantee. Durability is similarly challenged by inconsistent finality models, which can cause state confirmation discrepancies.

Decentralization is likewise limited in practice, as many interoperability solutions rely on TTPs, notary schemes, or federated validators, inherently reducing trust distribution [8]. The lack of standardized, quantifiable decentralization metrics further restricts rigorous evaluation and comparison across protocols.

5.1.3 Privacy-Preserving Mechanisms and Zero-Knowledge Proofs

Privacy-preserving properties such as unlinkability [16] remain underrepresented in blockchain interoperability research, despite their importance in mitigating the inherent transparency and traceability of blockchain systems. Cross-chain transactions often reuse metadata—such as addresses and transaction hashes—enabling activity correlation across networks. The absence of robust privacy mechanisms on even one participating blockchain can compromise unlinkability for the entire system.

Zero-knowledge proofs offer strong privacy guarantees but are challenging to implement in cross-chain protocols due to requiring advanced cryptographic setups—arithmetic circuit construction, trusted setup procedures, and high resource consumption for proof generation and verification. In heterogeneous blockchain environments, these challenges are compounded by the need to synchronize proof systems across differing architectures and cryptographic standards. The lack of standardized protocols for cross-chain zero-knowledge proof validation, along with potential compromise of the trusted setup, further hinders seamless deployment [25].

Zero-knowledge proofs must satisfy three core properties: completeness, soundness, and zero-knowledge [113]. Completeness ensures that a prover with valid knowledge can convince a verifier of a statement's truth; soundness prevents dishonest provers from convincing verifiers of false statements; and zero-knowledge ensures that no additional information is revealed beyond the truth of the statement. Achieving these consistently across heterogeneous blockchains is complex but essential for secure, trustless, and privacy-preserving cross-chain transactions.

5.1.4 Fragmented Threat Modeling and Attack Coverage

Notably, the majority of attack types—over 58%—were only analyzed in a single study. This limited coverage indicates that most existing research adopted a narrow threat model, potentially overlooking key vulnerabilities that have been exploited in real-world cross-chain attacks. While SPOF, DoS, and replay attacks have received slightly more attention, the lack of consistent analysis across other well-known vectors suggests a fragmented approach to security. The absence of comprehensive threat modeling across diverse interoperability mechanisms may leave systems exposed to less-studied but equally damaging attacks. This highlights a critical gap in the current literature and underscores the urgent need for future studies to adopt a more holistic and systematic approach to attack surface evaluation in cross-chain environments.

5.1.5 Quantum Computing Threats and Post-Quantum Cryptography

Quantum computing poses critical threats to blockchain and interoperability protocol security, particularly through Grover's and Shor's algorithms [114,115], which can break public-key cryptography and hash functions [23]. It also endangers authentication schemes in permissioned blockchains, where identity verification and access control are essential [116]. By compromising digital signatures and certificates, quantum attacks could enable unauthorized entities to impersonate participants, bypass access controls, and undermine network integrity [116]. To counter these risks, adopting post-quantum cryptosystems is essential for developing quantum-resistant blockchains and distributed ledger technologies [117].

Research should prioritize replacing vulnerable algorithms such as RSA and ECDSA with post-quantum alternatives, including lattice-based schemes like Dilithium [118] and Kyber [119], and hash-based schemes such as SPHINCS+ [120]. Integrating privacy-preserving techniques—such as ZK-STARKs and ZK-SNARKs—into post-quantum blockchain systems can further enhance privacy, authenticity, and regulatory compliance through selective disclosure [116]. The convergence of post-quantum cryptography and zero-knowledge proofs offers a promising pathway to building secure, privacy-preserving blockchain ecosystems in the post-quantum era.

5.1.6 Smart Contract Security in Cross-Chain Environments

Smart contracts in blockchain technology offer promising benefits but face critical security challenges, particularly in cross-chain environments. Errors or bugs in smart contracts can lead to vulnerabilities and attacks, resulting in asset loss and compromised trust [29]. Cross-chain smart contract invocations (CCSCIs) introduce additional interoperability and integration challenges due to the heterogeneity of blockchain protocols [34]. However, there is still a lack of clear methodologies for evaluating and validating smart contract quality and development processes [121], highlighting the critical nature of errors in cross-chain smart contracts.

5.1.7 Incentive Structures and Reputation Management

In parallel, the absence of robust incentive structures and reputation management systems presents a major barrier to secure and scalable adoption. Current interoperability protocols often lack effective incentive mechanisms for validators, leading to reduced participation and increased risks of misconduct. Additionally, robust reputation management systems are generally absent, making it difficult to assess and ensure the trustworthiness of nodes involved in cross-chain transactions. A dynamic reputation management system that adjusts trust indicators based on evolving blockchain trends is recommended.

5.1.8 Performance, Scalability, and Cost Trade-Offs

As blockchain ecosystems expand, the performance of interoperability mechanisms has become a critical concern due to the computational demands of many protocols [80,85]. Relay-based mechanisms offer strong security through continuous state verification, cryptographic proof generation, and cross-chain data synchronization, but these features introduce significant latency, high computational overhead, and reduced throughput—making relays costly and unsuitable for high-frequency or low-latency enterprise deployments [17,91].

Sidechain mechanisms improve flexibility and scalability but suffer from low throughput and high latency, largely due to the time-intensive two-way peg process, limiting their applicability in time-sensitive or large-scale enterprise contexts [122]. HTLC-based protocols enable trustless atomic swaps without intermediaries, yet their reliance on time-lock conditions causes delays and temporary fund lockups, reducing practicality for instant payments or high-volume trading [74].

Notary schemes provide faster transaction processing with minimal computational overhead, facilitating adoption in enterprise and permissioned networks, but they centralize trust among a small validator group, reducing decentralization [122]. Hybrid models aim to combine the security of relays with the flexibility of notaries or sidechains; however, they often increase architectural complexity, integration costs, and the attack surface [122].

A persistent gap lies in balancing security and efficiency. Protocols prioritizing strong security—such as relay-, sidechain-, and HTLC-based approaches—often face high latency, limited throughput, and heavy computational overhead, impeding large-scale or real-time use. Conversely, notary-based schemes deliver speed and efficiency but at the expense of decentralization and resilience, making them less suitable for high-assurance environments.

5.1.9 Real-World Deployment Barriers and Standardization Gaps

Designing interoperability protocols with minimal modifications to existing blockchain infrastructure is essential, particularly for permissioned blockchains and blockchain-based DApps. However, many protocols impose specific requirements that limit their applicability. For example, HTLC-based synchronization requires both blockchains to use the same hash function. Other protocols, such as Ethereum-based interoperability solutions, demand significant alterations to Ethereum's software, which may not be feasible for certain DApps. As a result, many cross-chain protocols face deployment challenges due to their dependence on underlying protocol modifications or restrictive trust models.

Practical barriers to real-world adoption include performance and scalability constraints. Current protocols often require significant optimization to achieve the throughput and latency necessary for enterprise-grade or real-time systems [77,60]. Underlying blockchain inefficiencies—such as consensus delays, cryptographic overhead, and architectural limitations—compound these issues. For instance, verifying a single Ethereum block header can require up to 64 million gas, making it prohibitively expensive [84]. Additional factors, including network traffic sensitivity [61], multi-step atomic swaps [83], and heavy cryptographic operations like BLS threshold signatures [58], further degrade performance. On-chain validation and proof generation can also increase operational costs [85,91].

Cross-chain compatibility and the absence of standards present further challenges. Some protocols demand strict prerequisites—such as matching hash functions [74] or specific source–target chain configurations [79]—while others require complex client modifications [58] or introduce maintenance-heavy governance structures [84]. Prototypes like InterTrust [59] lack integration with other blockchain systems, and many remain in early research phases without extensive performance testing or optimization [77].

Storage constraints, especially for IoT and edge devices, add to these hurdles, as maintaining complete transaction histories is impractical in resource-limited environments [73,88]. Addressing these challenges will require lightweight cryptographic schemes, standardized interoperability frameworks, and cost-efficient designs to ensure feasibility in diverse deployment contexts.

Although 71% of included studies were rated high quality in methodological assessments, most lacked fully operational implementations: 73% presented implementation results, 14% had no implementation, and 13% provided only proof-of-concept validation. This persistent gap between theoretical design and practical deployment underscores the need for more mature, deployable solutions.

5.1.10 Arbitrary Data Exchange beyond Asset Transfers

Researchers have proposed multiple interoperability mechanisms—sidechains, relays, HTLCs, and notary schemes—each with distinct technical constraints [123]. HTLCs are generally limited to simple asset exchanges [16], while sidechains face difficulties supporting more complex operations such as cross-chain smart contract invocation [9]. Notary schemes can enable richer scenarios, including data sharing and contract invocation, but often require strict authentication procedures that conflict with the privacy requirements of permissioned blockchains [11]. These challenges are compounded by the inherently restrictive nature of permissioned networks, where access is limited to authorized nodes [16].

Most protocols focus on asset transfers and event notifications, but sectors such as healthcare, supply chains, and education require secure, efficient arbitrary data exchange. Key barriers include the lack of standardized data schemas, formats, and verification procedures [33].

5.1.11 Emerging Technologies (AI, IoT, and Federated Learning)

Integrating blockchain, IoT, and AI can address key challenges such as data breaches, weak authentication, and centralization, particularly in sensitive sectors like healthcare [124–126]. Blockchain ensures data integrity, transparency, and secure device authentication [126,127], while smart contracts automate access control, enforce privacy policies, and maintain immutable audit trails [124,126]. Coupled with AI, blockchain-powered IoT networks enable real-time threat detection, predictive analytics, and autonomous decision-making [125,127].

Emerging approaches include lightweight consensus models like B-LPoET [1] to reduce cross-chain overhead, AI-based intrusion detection [4], and machine learning for IoT service classification [5]. Active learning models [128] and the B-AIQoE framework [129]—combining Ethereum with AI-enabled game-based learning—enhance content integrity, provenance, and secure delivery via smart contracts, offering capabilities transferable to permissioned blockchain interoperability. The fusion of blockchain and federated learning promises secure, scalable, and privacy-preserving IoT ecosystems [130]. However, IoT interoperability remains challenged by heterogeneous devices, protocols, and data formats. Integrating blockchain with 5G can enable decentralized, low-latency data exchange, while smart contracts support automated validation, authentication, and access control [131].

5.2 Future Research Directions

Future research and development on permissioned blockchain interoperability should focus on the following key areas:

- Comprehensive Security Evaluation: Current security assessments are narrow in scope, with most studies examining only a limited set of attack vectors and security properties. Future research should adopt holistic and standardized threat modeling approaches to ensure a complete understanding of potential vulnerabilities. While relay-based protocols have received relatively thorough analysis, HTLC- and notary-based systems remain underexamined. Comparative security studies across all major interoperability mechanisms are essential to achieve balanced insights and prevent overlooked risks.
- ACID Properties and Decentralization: Foundational properties such as atomicity, consistency, isolation, durability (ACID), and decentralization are underrepresented in the literature. Future work should explore practical strategies for enforcing these properties and develop standardized metrics to evaluate and benchmark decentralization across different protocols.
- Privacy Preservation: Greater emphasis is needed on privacy-enhancing technologies, particularly mechanisms for anonymity and unlinkability, which are often insufficiently addressed. Integrating advanced zero-knowledge proof systems (e.g., ZK-SNARKs, ZK-STARKs) into cross-chain environments is a promising direction.
- Post-Quantum Cryptography: Classical cryptographic algorithms such as RSA and ECDSA are vulnerable to quantum attacks. Future research should prioritize the adoption of quantum-resistant schemes, such as lattice-based algorithms (e.g., Dilithium, Kyber) and hash-based schemes (e.g., SPHINCS+).
- Smart Contract Security: Cross-chain smart contracts present unique security challenges due to heterogeneous environments. Formal verification frameworks, auditing tools, and standardized quality metrics are urgently required to reduce vulnerabilities and improve reliability.

- Real-World Applicability: Many existing interoperability protocols require significant modifications to existing blockchain infrastructures. Future studies should design lightweight, backward-compatible architectures to facilitate seamless integration with permissioned blockchain ecosystems.
- Incentive Mechanisms and Reputation Systems: The development of robust incentive structures and dynamic reputation management systems is needed to ensure validator reliability, prevent malicious behavior, and encourage active participation.
- Performance and Scalability Optimization: Protocol performance should be enhanced through off-chain computation, efficient cryptographic techniques, and reduced overhead to improve transaction throughput and lower operational costs. Dedicated experiments should evaluate scalability under varying transaction loads and network complexities.
- Stakeholder and Industry Collaboration: Engagement with the blockchain community, industry partners, and IoT device manufacturers is critical for guaranteeing that proposed solutions are practically viable and widely adoptable.
- Versatile Protocol Design: Future interoperability protocols should prioritize versatility and automation, enabling the secure and atomic execution of a wide range of operations, including asset transfers, data sharing, exchanges, and cross-chain smart contract invocations.

6 Conclusions

This systematic review provides a comprehensive examination of the current landscape of security and privacy in interoperability protocols for permissioned blockchains. By analyzing 56 peer-reviewed studies published between 2020 and 2025, the review identifies significant disparities in how different interoperability mechanisms address security and privacy concerns. Relay-based protocols show the broadest coverage of key properties and attack mitigations, whereas HTLC, notary schemes, and hybrid models often lack depth in their evaluations.

The findings reveal that 93% of reviewed studies assessed fewer than four security or attack dimensions, indicating a fragmented and narrow research focus. Moreover, critical features such as ACID properties, decentralization, and cross-chain attack resilience remain substantially underexplored. This gap poses risks to the reliability, integrity, and trustworthiness of blockchain-based systems increasingly deployed in sensitive and mission-critical domains.

To advance the field, future research should aim for more holistic and standardized security assessments across all interoperability mechanisms. This includes expanding the evaluation of underrepresented properties, systematically addressing a wider range of attack vectors, and validating proposed solutions in real-world deployments. Such efforts are essential to strengthen the foundational trust and robustness of cross-chain ecosystems in permissioned blockchain environments.

Acknowledgement: Not applicable.

Funding Statement: This work was supported by the International Scientific and Technological Cooperation Project of Huangpu and Development Districts in Guangzhou (2023GH17), the National Science and Technology Council in Taiwan under grant number NSTC-113-2224-E-027-001, Private Funding (PV009-2023), and the KW IPPP (Research Maintenance Fee) Individual/Centre/Group (RMF1506-2021) at Universiti Malaya, Malaysia. The funders had no role in study design, data collection and analysis, the decision to publish, or the preparation of the manuscript.

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization, Alsoudi Dua, Tan Fong Ang and Lip Yee Por; methodology, Alsoudi Dua and Tan Fong Ang; validation, Chin Soon Ku, Jiahui Chen and Uzair Aslam Bhatti; formal analysis, Alsoudi Dua, Tan Fong Ang, Chin Soon Ku, Okmi Mohammed, Yu Luo and Lip Yee Por; investigation, Chin Soon Ku and Lip Yee Por; resources, Jiahui Chen, Uzair Aslam Bhatti and Lip Yee Por;

data curation, Yu Luo; writing—original draft preparation, Alsoudi Dua, Tan Fong Ang and Lip Yee Por; writing—review and editing, Alsoudi Dua, Tan Fong Ang, Chin Soon Ku, Okmi Mohammed and Lip Yee Por; supervision, Tan Fong Ang and Lip Yee Por; project administration, Lip Yee Por. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article and its Supplementary Materials.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Supplementary Materials: The supplementary material is available online at https://www.techscience.com/doi/10.32604/cmc.2025.070413/s1. S1 Table: PRISMA 2020 Checklist; S2 Table: Assessment of Study Quality—MMAT Tool; S3 File: List of Excluded Studies; S4 File: List of Included and Excluded Studies; S5 Table: PRISMA 2020 for Abstracts Checklist.

References

1. Khan AA, Dhabi S, Yang J, Alhakami W, Bourouis S, Yee PL. B-LPoET: a middleware lightweight Proof-of-Elapsed Time (PoET) for efficient distributed transaction execution and security on Blockchain using multithreading technology. Comput Electr Eng. 2024;118(10):109343. doi:10.1016/j.compeleceng.2024.109343.
2. Mahmood Babur S, Ur Rehman Khan S, Yang J, Chen Y-L, Soon Ku C, Yee Por L. Preventing 51% attack by using consecutive block limits in bitcoin. IEEE Access. 2024;12(13):77852–69. doi:10.1109/ACCESS.2024.3407521.
3. Khan AA, Yang J, Laghari AA, Baqasah AM, Alroobaea R, Ku CS, et al. BAIoT-EMS: consortium network for small-medium enterprises management system with blockchain and augmented intelligence of things. Eng Appl Artif Intell. 2025;141:109838. doi:10.1016/j.engappai.2024.109838.
4. Sana L, Nazir MM, Yang J, Hussain L, Chen Y-L, Ku CS, et al. Securing the IoT cyber environment: enhancing intrusion anomaly detection with vision transformers. IEEE Access. 2024;12:82443–68. doi:10.1109/ACCESS.2024.3404778.
5. Abbasi MA, Chen Y-L, Khan AA, Memon ZA, Durrani NM, Yang J, et al. Enabling IoT service classification: a machine learning-based approach for handling classification issues in heterogeneous IoT services. IEEE Access. 2023;11:89024–37. doi:10.1109/ACCESS.2023.3306607.
6. Khan AA, Yang J, Awan SA, Baqasah AM, Alroobaea R, Chen Y-L, et al. Artificial intelligence, internet of things, and blockchain empowering future vehicular developments: a comprehensive multi-hierarchical lifecycle review. Hum-Centric Comput Inf Sci. 2025;15:13. doi:10.22967/HCIS.2025.15.013.
7. Shah D, Rani S, Shoukat K, Kalsoom H, Shoukat MU, Almujibah H, et al. Blockchain Factors in the design of smart-media for e-healthcare management. Sensors. 2024;24(21):6835. doi:10.3390/s24216835.
8. Wang G, Wang Q, Chen S. Exploring blockchains interoperability: a systematic survey. ACM Comput Surv. 2023;55(13s):1–38. doi:10.1145/3582882.
9. Ren K, Ho N-M, Loghin D, Nguyen T-T, Ooi BC, Ta Q-T, et al. Interoperability in blockchain: a survey. IEEE Trans Knowl Data Eng. 2023;35(12):12750–69. doi:10.1109/TKDE.2023.3275220.
10. Zhou L, Xiong X, Ernstberger J, Chaliasos S, Wang Z, Wang Y, et al. SoK: decentralized finance (DeFi) attacks. In: 2023 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA: IEEE; 2023. p. 2444–61. doi:10.1109/SP46215.2023.10179435.
11. Kotey SD, Tchao ET, Ahmed A, Agbemenu AS, Nunoo-Mensah H, Sikora A, et al. Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. IET Commun. 2023;17(8):891–914. doi:10.1049/cmu2.12594.
12. Han P, Yan Z, Ding W, Fei S, Wan Z. A survey on cross-chain technologies. Distributed Ledger Technol Res Pract. 2023;2(2):1–30. doi:10.1145/3573896.

13. Haugum T, Hoff B, Alsadi M, Li J. Security and privacy challenges in blockchain interoperability—a multivocal literature review. In: The International Conference on Evaluation and Assessment in Software Engineering 2022. New York, NY, USA: ACM; 2022. p. 347–56. doi:10.1145/3530019.3531345.
14. Duan L, Sun Y, Ni W, Ding W, Liu J, Wang W. Attacks against cross-chain systems and defense approaches: a contemporary survey. IEEE/CAA J Autom Sin. 2023;10(8):1647–67. doi:10.1109/JAS.2023.123642.
15. Mohammed MA, De-Pablos-Heredero C, Montes Botella JL. A systematic literature review on the revolutionary impact of blockchain in modern business. Appl Sci. 2024;14(23):11077. doi:10.3390/app142311077.
16. Yin R, Yan Z, Liang X, Xie H, Wan Z. A survey on privacy preservation techniques for blockchain interoperability. J Syst Archit. 2023;140(3):102892. doi:10.1016/j.sysarc.2023.102892.
17. Li W, Liu Z, Chen J, Liu Z, He Q. Towards blockchain interoperability: a comprehensive survey on cross-chain solutions. Blockchain Res Appl. 2025;100286. doi:10.1016/j.bcra.2025.100286.
18. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372:n71. doi:10.1136/bmj.n71.
19. Quan Nha H. Mixed Methods Appraisal Tool (MMAT) Version 8 n.d. [cited 2025 Mar 31]. Available from: http://mixedmethodsappraisaltoolpublic.pbworks.com/w/file/fetch/127916259/MMAT_2018_criteria-manual_2018-08-01_ENG.pdf.
20. Buterin V. Ethereum: a Next-generation smart contract and decentralized application platform (White paper); 2014. p. 1–36. [cited 2025 Mar 31]. Available from: https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.
21. Tripathi G, Ahad MA, Casalino G. A comprehensive review of blockchain technology: underlying principles and historical background with future challenges. Decis Anal J. 2023;9(1):100344. doi:10.1016/j.dajour.2023.100344.
22. Dong S, Abbas K, Li M, Kamruzzaman J. Blockchain technology and application: an overview. PeerJ Comput Sci. 2023;9(1):e1705. doi:10.7717/peerj-cs.1705.
23. Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access. 2020;8:21091–116. doi:10.1109/ACCESS.2020.2968985.
24. Zantalis F, Koulouras G, Karabetsos S. Blockchain technology: a framework for endless applications. IEEE Consum Electron Mag. 2024;13(2):61–71. doi:10.1109/MCE.2023.3248872.
25. Konkin A, Zapechnikov S. Zero knowledge proof and ZK-SNARK for private blockchains. J Comput Virol Hacking Tech. 2023;19(3):443–9. doi:10.1007/s11416-023-00466-1.
26. Ihle C, Trautwein D, Schubotz M, Meuschke N, Gipp B. Incentive mechanisms in peer-to-peer networks—a systematic literature review. ACM Comput Surv. 2023;55(14s):1–69. doi:10.1145/3578581.
27. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger fabric. In: Proceedings of the Thirteenth EuroSys Conference. New York, NY, USA: ACM; 2018. p. 1–15. doi:10.1145/3190508.3190538.
28. Cachin C. Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers. Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016). Chicago, IL, USA; 2016. p. 1–4. doi:10.1145/3211933.3211944.
29. Mollajafari S, Bechkoum K. Blockchain technology and related security risks: towards a seven-layer perspective and taxonomy. Sustainability. 2023;15(18):13401. doi:10.3390/su151813401.
30. Baliga A, Subhod I, Kamat P, Chatterjee S. Performance evaluation of the quorum blockchain platform. arXiv:1809.03421. 2018.
31. Brown RG. The corda platform: an introduction. Corda Platform White Paper: R3. 2018;1–21. [cited 2025 Jun 1]. Available from: https://r3.com/wp-content/uploads/2018/05/corda-platform-whitepaper.pdf.
32. Multichain-cross chain router protocol. Multichain. [cited 2025 Jun 1]. Available from: https://app.multichain.org/#/router.
33. Delgado-von-Eitzen C, Anido-Rifón L, Ruiz-Molina M, Fernández-Iglesias MJ. Bridging the gap: achieving seamless interoperability between ethereum-based blockchains using inter-blockchain communication protocols. Softw Pract Exp. 2025. doi:10.1002/spe.70008.

34. Falazi G, Breitenbücher U, Leymann F, Schulte S. Cross-chain smart contract invocations: a systematic multi-vocal literature review. ACM Comput Surv. 2024;56(6):1–38. doi:10.1145/3638045.
35. Kwon J, Buchman E. Cosmos Whitepaper: a network of distributed ledgers [Internet]. Cosmos Network. 2017;1–31. [cited 2025 Jun 1]. Available from: https://cosmos.network/whitepaper/.
36. Wood G. Polkadot: vision for a heterogeneous multi-chain framework. White Paper. 2016;21:4662.
37. Verdian G, Tasca P, Paterson C, Mondelli G. Quant Overledger: Whitepaper v0.1. Technical Report. London, UK: UCL Discovery; 2018.
38. Thorchain. [cited 2025 Jul 31]. Available from: https://thorchain.org/.
39. Gusenbauer M, Haddaway NR. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. Res Synth Methods. 2020;11(2):181–217. doi:10.1002/jrsm.1378.
40. Correia PHB, Marques MA, Simplicio MA, Ermlivitch L, Miers CC, Pillon MA. Comparative analysis of permissioned blockchains: cosmos, hyperledger fabric, quorum, and XRPL. In: 2024 IEEE International Conference on Blockchain (Blockchain). Copenhagen, Denmark: IEEE; 2024. p. 464–9. doi:10.1109/Blockchain62396.2024.00068.
41. Hossain D, Mamun Q, Islam R. Unleashing the potential of permissioned blockchain: addressing privacy, security, and interoperability concerns in healthcare data management. Electronics. 2024;13(24):5050. doi:10.3390/electronics13245050.
42. Kraus S, Breier M, Dasí-Rodríguez S. The art of crafting a systematic literature review in entrepreneurship research. Int Entrep Manag J. 2020;16(3):1023–42. doi:10.1007/s11365-020-00635-4.
43. Belchior R, Süßenguth J, Feng Q, Hardjono T, Vasconcelos A, Correia M. A brief history of blockchain interoperability. Commun ACM. 2024;67(10):62–9. doi:10.1145/3648607.
44. Mohamed Shaffril HA, Samsuddin SF, Abu Samah A. The ABC of systematic literature review: the basic methodological guidance for beginners. Qual Quant. 2021;55(4):1319–46. doi:10.1007/s11135-020-01059-6.
45. Nussbaumer-Streit B, Klerings I, Dobrescu AI, Persad E, Stevens A, Garritty C, et al. Excluding non-English publications from evidence-syntheses did not change conclusions: a meta-epidemiological study. J Clin Epidemiol. 2020;118(5):42–54. doi:10.1016/j.jclinepi.2019.10.011.
46. Donthu N, Kumar S, Mukherjee D, Pandey N, Lim WM. How to conduct a bibliometric analysis: an overview and guidelines. J Bus Res. 2021;133(5):285–96. doi:10.1016/j.jbusres.2021.04.070.
47. Lindgren BM, Lundman B, Graneheim UH. Abstraction and interpretation during the qualitative content analysis process. Int J Nurs Stud. 2020;108(3):103632. doi:10.1016/j.ijnurstu.2020.103632.
48. Love J, Selker R, Marsman M, Jamil T, Dropmann D, Verhagen J, et al. JASP: graphical statistical software for common statistical designs. J Stat Softw. 2019;88. doi:10.18637/jss.v088.i02.
49. van Doorn J, van den Bergh D, Böhm U, Dablander F, Derks K, Draws T, et al. The JASP guidelines for conducting and reporting a Bayesian analysis. Psychon Bull Rev. 2021;28(3):813–26. doi:10.3758/s13423-020-01798-5.
50. Pawczuk L, Walker R, Tanco CC. Deloitte's 2021 global blockchain survey: financial leaders see digital assets as the future. Deloitte Insights; 2021. [cited 2025 Jun 1]. Available from: https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html.
51. Borasi P. Blockchain distributed ledger market expected to reach $137.29 billion by 2027. Allied Market Research 2021. [cited 2025 Jun 1]. Available from: https://www.alliedmarketresearch.com/press-release/blockchain-distributed-ledger-market.html#:~:text=According%20to%20a%20recent%20report,at%20%242.89%20billion%20in%202019%2C.
52. Augusto A, Belchior R, Correia M, Vasconcelos A, Zhang L, Hardjono T. SoK: security and privacy of blockchain interoperability. In: 2024 IEEE Symposium on Security and Privacy (SP). San Francisco, CA, USA: IEEE; 2024. p. 3840–65. doi:10.1109/SP54263.2024.00255.
53. Ronin bridge. Chainlink CCIP. [cited 2025 Jun 1]. Available from: https://bridge.roninchain.com/.
54. Polybridge. Polynetwork. [cited 2025 Jun 1]. Available from: https://bridge.poly.network/testnet.
55. Binanc. BNB Chain. [cited 2025 Jun 1]. Available from: https://www.binance.org/.
56. Portal token bridge. Portal Wormhole. [cited 2025 Jun 1]. Available from: https://portalbridge.com/.

57. Ghosh BC, Bhartia T, Addya SK, Chakraborty S. Leveraging public-private blockchain interoperability for closed consortium interfacing. In: IEEE INFOCOM 2021—IEEE Conference on Computer Communications. Vancouver, BC, Canada: IEEE; 2021. p. 1–10. doi:10.1109/INFOCOM42981.2021.9488683.
58. Robinson P, Ramesh R, Johnson S. Atomic crosschain transactions for ethereum private sidechains. Blockchain: Res Appl. 2022;3(1):100030. doi:10.1016/j.bcra.2021.100030.
59. Wang G, Nixon M. InterTrust: towards an efficient blockchain interoperability architecture with trusted services. In: 2021 IEEE International Conference on Blockchain (Blockchain). Melbourne, Australia: IEEE; 2021. p. 150–9. doi:10.1109/Blockchain53845.2021.00029.
60. Vishwakarma L, Kumar A, Das D. CrossLedger: a pioneer cross-chain asset transfer protocol. In: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid). Bangalore, India: IEEE; 2023. p. 568–78. doi:10.1109/CCGrid57682.2023.00059.
61. Bu G, Haouara R, Nguyen T-S-L, Potop-Butucaru M. Cross hyperledger fabric transactions. In: Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems. New York, NY, USA: ACM; 2020. p. 35–40. doi:10.1145/3410699.3413796.
62. Darshan M, Amet M, Srivastava G, Crichigno J. An architecture that enables cross-chain interoperability for next-gen blockchain systems. IEEE Internet Things J. 2023;10(20):18282–91. doi:10.1109/JIOT.2023.3279693.
63. Li D, Ding P, Zhou Y, Yang Y, Li C. Secure, efficient, and privacy-protecting one-to-many cross-chain shared data consistency audit. In: 2023 IEEE International Conference on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom). Wuhan, China: IEEE; 2023. p. 64–71. doi:10.1109/ISPA-BDCloud-SocialCom-SustainCom59178.2023.00041.
64. Yin Z, Zhang B, Xu J, Lu K, Ren K. Bool network: an open, distributed, secure cross-chain notary platform. IEEE Trans Inf Forensics Secur. 2022;17:3465–78. doi:10.1109/TIFS.2022.3209546.
65. Li T, Niu P, Wang Y, Zeng S, Wang X, Susilo W. HT2REP: a fair cross-chain atomic exchange protocol under UC framework based on HTLCs and TRE. Comput Stand Interfaces. 2024;89(37):103834. doi:10.1016/j.csi.2024.103834.
66. Belchior R, Vasconcelos A, Correia M, Hardjono T. Hermes: fault-tolerant middleware for blockchain interoperability. Future Gener Comput Syst. 2022;129(6):236–51. doi:10.1016/j.future.2021.11.004.
67. Hei Y, Li D, Zhang C, Liu J, Liu Y, Wu Q. Practical AgentChain: a compatible cross-chain exchange system. Future Gener Comput Syst. 2022;130(9):207–18. doi:10.1016/j.future.2021.11.029.
68. Jiang J, Zhang Y, Zhu Y, Dong X, Wang L, Xiang Y. DCIV: decentralized cross-chain data integrity verification with blockchain. J King Saud Univ-Comput Inf Sci. 2022;34(10):7988–99. doi:10.1016/j.jksuci.2022.07.015.
69. Zhang Y, Jiang J, Dong X, Wang L, Xiang Y. BeDCV: blockchain-enabled decentralized consistency verification for cross-chain calculation. IEEE Trans Cloud Comput. 2023;11(3):2273–84. doi:10.1109/TCC.2022.3196937.
70. Robinson P, Ramesh R. General purpose atomic crosschain transactions. In: 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). Paris, France: IEEE; 2021. p. 61–8. doi:10.1109/BRAINS52497.2021.9569837.
71. Lee Y, Son B, Jang H, Byun J, Yoon T, Lee J. Atomic cross-chain settlement model for central banks digital currency. Inf Sci. 2021;580(5):838–56. doi:10.1016/j.ins.2021.09.040.
72. Barbara F, Schifanella C. BxTB: cross-chain exchanges of bitcoins for all Bitcoin wrapped tokens. In: 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA). San Antonio, TX, USA: IEEE; 2022. p. 143–50. doi:10.1109/BCCA55292.2022.9922019.
73. Zhao J, Zhang Y, Jiang J, Hua Z, Xiang Y. A secure dynamic cross-chain decentralized data consistency verification model. J King Saud Univ-Comput Inf Sci. 2024;36(1):101897. doi:10.1016/j.jksuci.2023.101897.
74. Barbàra F, Schifanella C. MP-HTLC: enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract. Concurr Comput. 2023;35(9):1128. doi:10.1002/cpe.7656.
75. Sanchez A, Stewart A, Shirazi F. Bridging sapling: private cross-chain transfers. In: 2022 IEEE Crosschain Workshop (ICBC-CROSS). Shanghai, China: IEEE; 2022. p. 1–9. doi:10.1109/ICBC-CROSS54895.2022.9793325.
76. Zhang S, Zhou R, Wang L, Xu S, Shao W. Cross-chain asset transaction method based on ring signature for identity privacy protection. Electronics. 2023;12(24):5010. doi:10.3390/electronics12245010.

77. Liang X, Zhao Y, Wu J, Yin K. A privacy protection scheme for cross-chain transactions based on group signature and relay chain. Int J Digit Crime Forensics. 2022;14(2):1–20. doi:10.4018/IJDCF.302876.
78. Li Y, Weng J, Li M, Wu W, Weng J, Liu J-N, et al. ZeroCross: a sidechain-based privacy-preserving cross-chain solution for Monero. J Parallel Distrib Comput. 2022;169(8):301–16. doi:10.1016/j.jpdc.2022.07.008.
79. Kiayias A, Zindros D. Proof-of-work sidechains. In: Financial cryptography and data security; 2020. Vol. 11599, p. 21–34. doi:10.1007/978-3-030-43725-1_3.
80. Lei L, Song L, Wan J. Improved method of blockchain cross-chain consensus algorithm based on weighted PBFT. Comput Intell Neurosci. 2022;2022(3):1–9. doi:10.1155/2022/5169259.
81. Guo H, Liang H, Huang J, Ou W, Han W, Zhang Q, et al. A framework for efficient cross-chain token transfers in blockchain networks. J King Saud Univ-Comput Inf Sci. 2024;36(2):101968. doi:10.1016/j.jksuci.2024.101968.
82. Abbas H, Caprolu M, Di Pietro R. Analysis of Polkadot: architecture, internals, and contradictions. In: 2022 IEEE International Conference on Blockchain (Blockchain). Espoo, Finland: IEEE; 2022. p. 61–70. doi:10.1109/Blockchain55522.2022.00019.
83. Dwivedi R, Singla T, Shukla S. Cross-chain atomic swaps without time locks. In: 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA). Kuwait, Kuwait: IEEE; 2023. p. 606–14. doi:10.1109/BCCA58897.2023.10338878.
84. Xie T, Zhang J, Cheng Z, Zhang F, Zhang Y, Jia Y, et al. zkBridge. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM; 2022. p. 3003–17. doi:10.1145/3548606.3560652.
85. Westerkamp M, Diez M. Verilay: a verifiable proof of stake chain relay. In: 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). Shanghai, China: IEEE; 2022. p. 1–9. doi:10.1109/ICBC54727.2022.9805554.
86. Wu Z, Xiao Y, Zhou E, Pei Q, Wang Q. A solution to data accessibility across heterogeneous blockchains. In: 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). Hong Kong, China: IEEE; 2020. p. 414–21. doi:10.1109/ICPADS51040.2020.00062.
87. Xu Y, He R, Dai S, Zhang Y. ChainKeeper: a cross-chain scheme for governing the chain by chain. IET Blockchain. 2023;3(4):249–64. doi:10.1049/blc2.12047.
88. de Vos M, Ileri CU, Pouwelse J. XChange: a universal mechanism for asset exchange between permissioned blockchains. World Wide Web. 2021;24(5):1691–728. doi:10.1007/s11280-021-00870-x.
89. Liu W, Wu H, Meng T, Wang R, Wang Y, Xu C-Z. AucSwap: a Vickrey auction modeled decentralized cross-blockchain asset transfer protocol. J Syst Archit. 2021;117(4):102102. doi:10.1016/j.sysarc.2021.102102.
90. Chen K, Lee L-F, Chiu W, Su C, Yeh K-H, Chao H-C. A trusted reputation management scheme for cross-chain transactions. Sensors. 2023;23(13):6033. doi:10.3390/s23136033.
91. Sober M, Scaffino G, Spanring C, Schulte S. A voting-based blockchain interoperability oracle. In: 2021 IEEE International Conference on Blockchain (Blockchain). Melbourne, Australia: IEEE; 2021. p. 160–9. doi:10.1109/Blockchain53845.2021.00030.
92. Zhang S, Xie T, Gai K, Xu L. ARC: an asynchronous consensus and relay chain-based cross-chain solution to consortium blockchain. In: 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom). Xi’an, China: IEEE; 2022. p. 86–92. doi:10.1109/CSCloud-EdgeCom54986.2022.00024.
93. Sun Y, Yi L, Duan L, Wang W. A Decentralized cross-chain service protocol based on notary schemes and hash-locking. In: 2022 IEEE International Conference on Services Computing (SCC). Barcelona, Spain: IEEE; 2022. p. 152–7. doi:10.1109/SCC55611.2022.00033.
94. Zhang Y, Wang Z, Wang Y, Liu X, Hei X. Cross-chain jamming attack with light client verification clash in IBC protocol. In: 2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS). Chongqing, China: IEEE; 2022. p. 150–8. doi:10.1109/IUCC-CIT-DSCI-SmartCNS57392.2022.00034.
95. Xiong A, Liu G, Zhu Q, Jing A, Loke SW. A notary group-based cross-chain mechanism. Digit Commun Netw. 2022;8(6):1059–67. doi:10.1016/j.dcan.2022.04.012.

96. Cheng L, Lv Z, Alfarraj O, Tolba A, Yu X, Ren Y. Secure cross-chain interaction solution in multi-blockchain environment. Heliyon. 2024;10(7):e28861. doi:10.1016/j.heliyon.2024.e28861.
97. Lv Z, Wu D, Yang W, Duan L. Attack and protection schemes on fabric isomorphic crosschain systems. Int J Distrib Sens Netw. 2022;18(1):155014772110599. doi:10.1177/15501477211059945.
98. Tian H, Ruan Z, Fan Z. A Cross-chain mechanism based on hierarchically managed notary group. Int J Adv Comput Sci Appl. 2025;16(4). doi:10.14569/IJACSA.2025.0160450.
99. Huang Q, Tan M, Tian W. Cross-chain identity authentication method based on relay chain. Information. 2025;16(1):27. doi:10.3390/info16010027.
100. Li T, Huang H, Abla P, Deng Z, Yang Q, Xie A, et al. DataFly: a confidentiality-preserving data migration across heterogeneous blockchains. IEEE Trans Comput. 2025;74(6):1814–28. doi:10.1109/TC.2025.3535830.
101. Wu Z, Wang Y, Wang L. GAM: a scalable and efficient multi-chain data sharing scheme. Inf Process Manag. 2025;62(3):104004. doi:10.1016/j.ipm.2024.104004.
102. Li M, Weng J, Li Y, Wu Y, Weng J, Li D, et al. IvyCross: a privacy-preserving and concurrency control framework for blockchain interoperability. IEEE Trans Dependable Secure Comput. 2015;1–22. doi:10.1109/tmc.2025.3562875.
103. Jiang J, Zhang Y, Zhao J, Gao L, Zhu L, Tian Z. Towards efficient consistency auditing of dynamic data in cross-chain interaction. IEEE Trans Dependable Secure Comput. 2025;2025(4):1–13. doi:10.1109/TDSC.2025.3532320.
104. Si H, Li W, Su N, Li T, Li Y, Zhang C, et al. A cross-chain access control mechanism based on blockchain and the threshold Paillier cryptosystem. Comput Commun. 2024;223(2):68–80. doi:10.1016/j.comcom.2024.05.012.
105. Wang Y, Yan Y, Liu X, Gao W, Wang Z. A technique for ensured cross chain IBC transactions using TPM. In: 2024 2nd International Conference on Big Data and Privacy Computing (BDPC). Macau, China: IEEE; 2024. p. 82–90. doi:10.1109/BDPC59998.2024.10649356.
106. Khorasani KE, Rouhani S, Pan R, Pourheidari V. Automated gateways: a smart contract-powered solution for interoperability across blockchains. In: 2024 IEEE International Conference on Blockchain (Blockchain). Copenhagen, Denmark: IEEE; 2024. p. 611–8. doi:10.1109/Blockchain62396.2024.00090.
107. Li D, Xu S, He H, Xue H. Cross-chain transaction tracking protocol based on multi-dimensional digital watermarking fingerprints. In: 2024 6th International Conference on Frontier Technologies of Information and Computer (ICFTIC). Qingdao, China: IEEE; 2024. p. 265–9. doi:10.1109/ICFTIC64248.2024.10913002.
108. Cai Y, Cheng R, Zhou Y, Zhang S, Xiao J, Jin H. Enabling complete atomicity for cross-chain applications through layered state commitments. In: 2024 43rd International Symposium on Reliable Distributed Systems (SRDS). Charlotte, NC, USA: IEEE; 2024. p. 248–59. doi:10.1109/SRDS64841.2024.00032.
109. Lou L, He W, Tang X, Yang Y, Zhang T, Cheng Y, et al. Enabling trustable financing: a verifiable privacy-preserving cross-chain protocol. In: 2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops). Hangzhou, China: IEEE; 2024. p. 214–9. doi:10.1109/ICCCWorkshops62562.2024.10693771.
110. Mao H, Nie T, Yu M, Dong X, Li X, Yu G. SMPTC3: secure multi-party protocol based trusted cross-chain contracts. Mathematics. 2024;12(16):2562. doi:10.3390/math12162562.
111. Liang X, Chen J, Du R. XPull: a relay-based blockchain intercommunication framework achieving cross-chain state pulling. Chin J Electron. 2024;33(5):1261–73. doi:10.23919/cje.2023.00.004.
112. Guo Y, Xu M, Cheng X, Yu D, Qiu W, Qu G, et al. zkCross: a novel architecture for cross-chain privacy-preserving auditing. In: Proceedings of the 33rd USENIX Conference on Security Symposium. USA: USENIX Association; 2024. p. 6219–35.
113. Partala J, Nguyen TH, Pirttikangas S. Non-interactive zero-knowledge for blockchain: a survey. IEEE Access. 2020;8:227945–61. doi:10.1109/ACCESS.2020.3046025.
114. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, NM, USA: IEEE; 1994. p. 124–34. doi:10.1109/SFCS.1994.365700.
115. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the Annual ACM Symposium on Theory of Computing. New York, NY, USA: ACM; 1996. p. 212–9. doi:10.1145/237814.237866.
116. Bugra Sezer B, Akleylek S, Nuriyev U. PP-PQB: privacy-preserving in post-quantum blockchain-based systems: a systematization of knowledge. IEEE Access. 2025;13:41382–405. doi:10.1109/ACCESS.2025.3545943.

117. Giusto E, Vakili MG, Gandino F, Demartini C, Montrucchio B. Quantum pliers cutting the blockchain. IT Prof. 2020;22(6):90–6. doi:10.1109/MITP.2020.2974690.

118. Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, et al. Crystals-dilithium: a lattice-based digital signature scheme. IACR Trans Cryptogr Hardw Embed Syst. 2018;2018:238–68. doi:10.13154/tches.v2018.i1.238-268.

119. Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, et al. CRYSTALS -Kyber: a CCA-secure module-lattice-based KEM. In: 2018 IEEE European Symposium on Security and Privacy (Euro S & P). London, UK: IEEE; 2018. p. 353–67. doi:10.1109/EuroSP.2018.00032.

120. Bernstein DJ, Niederhagen R, Hülsing A, Rijneveld J, Kölbl S, Schwabe P. The SpHiNCS+ signature framework. In: Proceedings of the ACM Conference on Computer and Communications Security. New York, NY, USA: ACM; 2019. p. 2129–46. doi:10.1145/3319535.3363229.

121. Sanchez-Gomez N, Torres-Valderrama J, Garcia-Garcia JA, Gutierrez JJ, Escalona MJ. Model-based software design and testing in blockchain smart contracts: a systematic literature review. IEEE Access. 2020;8:164556–69. doi:10.1109/ACCESS.2020.3021502.

122. Yuan H, Fei S, Yan Z. Technologies of blockchain interoperability: a survey. Digit Commun Netw. 2025;11(1):210–24. doi:10.1016/j.dcan.2023.07.008.

123. Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: past, present, and future trends. ACM Comput Surv. 2022;54(8):1–41. doi:10.1145/3471140.

124. Obaidat MA, Rawashdeh M, Alja'afreh M, Abouali M, Thakur K, Karime A. Exploring IoT and blockchain: a comprehensive survey on security, integration strategies, applications and future research directions. Big Data Cogn Comput. 2024;8(12):174. doi:10.3390/bdcc8120174.

125. Al Karkouri A, Oughannou Z, El Gannour O, Mzili T, Bourekkadi S. Internet of things for smart building security: leveraging a blockchain for enhanced IoT security. Mesop J CyberSecur. 2025;5(1):187–201. doi:10.58496/MJCS/2025/013.

126. Alam S, Bhatia S, Shuaib M, Khubrani MM, Alfayez F, Malibari AA, et al. An overview of blockchain and IoT integration for secure and reliable health records monitoring. Sustainability. 2023;15(7):5660. doi:10.3390/su15075660.

127. Alharbi S, Attiah A, Alghazzawi D. Integrating blockchain with artificial intelligence to secure IoT networks: future trends. Sustainability. 2022;14(23):16002. doi:10.3390/su142316002.

128. Yang J, Qin H, Wang J, Yee PL, Prajapat S, Kumar G, et al. IoT-driven skin cancer detection: active learning and hyperparameter optimization for enhanced accuracy. IEEE J Biomed Health Inform. 2025;2025:1–11. doi:10.1109/JBHI.2025.3578419.

129. Wagan AA, Khan AA, Chen Y-L, Yee PL, Yang J, Laghari AA. Artificial intelligence-enabled game-based learning and quality of experience: a novel and secure framework (B-AIQoE). Sustainability. 2023;15(6):5362. doi:10.3390/su15065362.

130. Gupta M, Kumar M, Dhir R. Unleashing the prospective of blockchain-federated learning fusion for IoT security: a comprehensive review. Comput Sci Rev. 2024;54(05):100685. doi:10.1016/j.cosrev.2024.100685.

131. Abhang D, Ghule S. Interoperability of blockchain technology in 5G enabled IoT. Int J Creat Res Thoughts. 2021;9:2899–905.