SoK: Security and Privacy of Blockchain Interoperability

André Augusto*† Rafael Belchior*† Miguel Correia*† André Vasconcelos*† Luyao Zhang‡ Thomas Hardjono§
*INESC-ID †Instituto Superior Técnico ‡Duke Kunshan University §MIT Connection Science

2024 IEEE Symposium on Security and Privacy (SP) | 979-8-3503-3130-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/SP54263.2024.00255

***Abstract*—Recent years have witnessed significant advancements in cross-chain technology. However, the field faces two pressing challenges. On the one hand, hacks on cross-chain bridges have led to monetary losses of around 3.1 billion USD, highlighting flaws in security models governing interoperability mechanisms and the ineffectiveness of incident response frameworks. On the other hand, users and bridge operators experience restricted privacy, which broadens the potential attack surface.**

In this paper, we present the most comprehensive study to date on the security and privacy of blockchain interoperability. We employ a systematic literature review, yielding a corpus of 212 relevant documents, including 58 academic papers and 154 gray literature documents, out of a pool of 531 results. We systematically categorize 57 interoperability solutions based on a novel security and privacy taxonomy. Our dataset, comprising academic research, disclosures from bug bounty programs, and audit reports, exposes 45 cross-chain vulnerabilities, 4 privacy leaks, and 92 mitigation strategies. Leveraging this data, we analyze 18 notable bridge hacks accounting for over 2.9 billion USD in losses, mapping them to the identified vulnerabilities.

Our findings reveal that a substantial portion (65.8%) of stolen funds originates from projects secured by intermediary permissioned networks with unsecured cryptographic key operations. Privacy-wise, we demonstrate that achieving unlinkability in cross-chain transactions is contingent on the underlying ledgers providing some form of confidentiality. Our study offers 17 critical insights into the security and privacy of cross-chain systems. We pinpoint promising future research directions, underscoring the urgency of enhancing security and privacy efforts in cross-chain technology. The identified improvements have the potential to mitigate the financial risks associated with bridge hacks, fostering user trust in the blockchain ecosystem and, consequently, wider adoption.

Keywords: Cross-chain, Security, Privacy, Vulnerabilities, Blockchain Technology, Cryptocurrency, Financial Losses, Systematic Literature Review, Taxonomy, Mitigations.

∗. The first two authors contributed equally to this work. Rafael conducted this research while at MIT Connection Science supported by a Fulbright Scholarship.

†. Contact André Augusto (andre.augusto@tecnico.ulisboa.pt), Rafael Belchior (rafael.belchior@tecnico.ulisboa.pt), Miguel Correia (miguel.p.correia@tecnico.ulisboa.pt) and André Vasconcelos (andre.vasconcelos@tecnico.ulisboa.pt) at INESC-ID and Técnico Lisboa; Contact Luyao Zhang (lz183@duke.edu) at Duke Kunshan University; Contact Thomas Hardjono (hardjono@mit.edu) at MIT Connection Science.

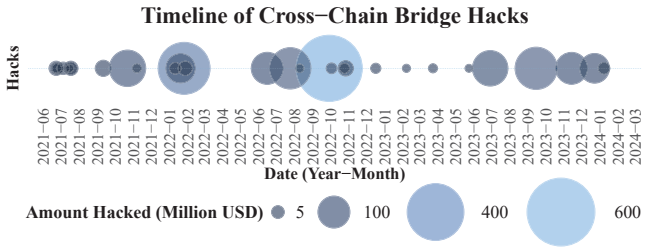

Figure 1. Timeline of cross-chain bridge hacks from May 2021 to February 2024. The dataset includes 33 bridge hacks amounting to over 3.2 billion USD.

1. Introduction

Blockchain interoperability is paramount for realizing the full potential of blockchain technology. As the landscape evolves, interoperability is gaining momentum in use cases such as bridging liquidity fragmentation, optimizing decentralized exchange (DEX) trades, enhancing scalability through sharding [1], expanding through sidechains [2], and enabling asset exchanges and transfers across platforms [3]. Stepping back to 1996, Wegner stated that "interoperability is the ability of two or more software components to cooperate despite differences in language, interface, and execution platforms" [4]. However, achieving interoperability across blockchains – distributed systems where mutual trust is often absent – adds a dimension of complexity. Here, the challenge is not simply to sync *n* software components but rather to integrate *n* distributed systems, each with its unique challenges, encompassing safety, liveness, accountability, and centralization [5], [6]. Such orchestration is performed by interoperability mechanisms (IMs) [7]. The different transactional models, consensus mechanisms, and cryptographic primitives in the networks escalate this challenge. Despite these challenges, the domain has seen prolific contributions from scholars, providing solutions, novel architectures, and varied use cases [8]–[16]. A recurring theme in these studies underscores the pressing need for rigorous research on IM security and privacy.

The secure interoperation of different blockchains involves establishing a new security boundary that depends on the security of at least two existing networks and involves multiple design trade-offs [12], [17]–[19]. Simultaneously, the disclosure of cross-chain transactions might be sensitive and can reveal much about the entities holding the data or the data itself [20]–[22]. We underline that striking a balance

DOI 10.1109/SP54263.2024.00182

between security and privacy is a must. While privacy is essential, accountability is equally necessary to deter and penalize misconduct and maintain protocol fairness.

Since May 2021, mounting losses due to bridge hacks have exceeded 3.1B USD and have been recurrent since then (cf. Figure 1). According to Immunefi [23], white-hat hackers have been compensated over 20M USD through bug bounty programs, preventing potential losses of a staggering 1B USD. Moreover, cross-chain bridge hacks have raised to the top of the DeFi incidents leaderboard [24]–[26], emerging as the preferred target of cybercriminals. The present scenario, as of mid-2023, paints a grim picture with rampant hacks [27]–[30]. Consequently, the total value locked (TVL) in cross-chain bridges has nose-dived from its zenith at 58B USD in early 2022 to a mere 5.5B USD in December 2023, a downfall also attributed to the decrease in asset prices in the bearish market [31], [32]. We hypothesize that intertwined cross-chain systems, in conjunction with already well-studied vulnerability-prone smart contracts, be it in bytecode or higher-level language dimensions [33], have amplified the risk exposure of these protocols. Due to the large amounts of funds involved, these protocols are attractive honeypots for attackers, making them highly sought-after targets in the three interoperability modes we examine: asset exchanges, asset transfers, and data transfers [19], [34].

1.1. Research Questions and Contributions

In this paper, we systematize knowledge about the security and privacy of blockchain interoperability solutions. So far, this information has been scattered among multiple unstructured and sometimes unidentified sources. To achieve this goal, in Section 2, we first provide the relevant background knowledge on blockchain interoperability necessary to understand this work. Then, we provide three contributions answering a specific research question (RQ), pointing to a relevant section discussing it.

RQ1: What are the different security- and privacy-centric goals used in blockchain interoperability, and what are the technical building blocks that guarantee them? Security-wise, we **define a set of properties** inspired by the distributed system literature and **explore relevant** security **approaches** used to ensure safety and liveness for each IM. In terms of privacy, we analyze the existing privacy-enabling approaches for IMs and categorize them according to the guarantees of user and bridge operator anonymity, confidentiality of transactional data, and unlinkability of transactions across multiple blockchains. We present a **systematization of knowledge** comparing 57 IMs based on the relevant properties and approaches defined. Over half (54%) of the classified papers have been published since 2022, highlighting the timeliness of this work. Sections 3 and 4.1 answer this RQ.

RQ2: What are the cross-chain vulnerabilities, attack vectors, privacy leaks, and mitigations currently known, and how are they mapped to past incidents? Our third research inquiry requires us to investigate cross-chain attacks and privacy leaks in the literature, focusing on the vulnerabilities that made them possible. We categorize 45 identified vulnerabilities into four distinct security layers (cf. Section 3.1) and present 4 privacy leaks. We identify possible mitigations to all vulnerabilities and leaks. We also **foster synergies between academia and industry** by examining 18 cross-chain hacks that account for more than 2.9B USD hacked and comparing them with the theoretical vulnerabilities found in academic research. We pinpoint the disparities between the existing research findings and their practical application by providing additional 6 **strategic insights**. Section 4.2 answers this RQ.

RQ3: Based on the existing gaps, what are potential best practices and avenues for future research to enhance the security and privacy of cross-chain protocols? In a time when the industry is actively seeking stability, we observe that the design of cross-chain solutions remains largely ad hoc, with each solution custom-crafted for specific blockchains or applications. Through a comprehensive analysis of existing studies, we present a collection of **best practices and future research avenues**. We provide initial insights that protocol designers, developers, and analysts can use as a foundation for further research and development. Sections 4.3 and 4.4 answer this RQ.

Finally, Sections 5 and 6 briefly discuss the contribution to related literature and present our forward-looking remarks and insights, respectively.

1.2. Research Methodology

To address the research questions, we structure our methodology into two phases. Firstly, we crawled papers from 2015 using the Google Scholar keyword search. Secondly, due to the unstructured practices in the area, we included multiple gray literature resources focusing on past cross-chain hacks, audit reports, vulnerabilities, and disclosures through bug bounty programs. In total, we analyzed 242 relevant documents, 58 from Google Scholar, 111 from snowballing, forward reference search, and by setting up Google alerts, 10 audit reports from reputable entities such as *Certik*, *Chainsecurity*, *Consensys*, *Halborn* and *Trail of Bits*, and 63 additional gray literature documents. A more thorough description of the methodology is presented in Appendix B.

Data and Code Availability: The data and code for ensuring replicability are available on GitHub, accessible at the following URL: https://github.com/RafaelAPB/SoKSPBlockchainInterop.

2. A Primer on Blockchain Interoperability

Blockchain interoperability allows data and value to flow across different domains and is facilitated by an IM. The domains under focus in this paper are distributed ledgers $\{l_1, l_2, ..., l_k\}$. The IM can be designed and deployed in multiple ways, depending on the required guarantees (e.g., centralized or decentralized, distributed or non-distributed).

2.1. Interoperability Modes

The literature [1], [7], [34]–[37] agrees on the existence of three modes of interoperability: **asset exchanges (AE)**, **data transfers (DT)**, and **asset transfers (AT)**. Different interoperation modes require distinct protocol architectures, providing different security and privacy guarantees.

Consider accounts $\mathcal{A}_1$ and $\mathcal{A}_2$ in ledgers l_1 and l_2, respectively. Asset exchange protocols allow untrusted parties to exchange assets in different networks. For example, asset X owned by $\mathcal{A}_1$ on l_1, can be exchanged for asset Y owned by $\mathcal{A}_2$ on l_2. At the end, $\mathcal{A}_2$ owns X on l_1, and $\mathcal{A}_1$ owns Y on l_2. An asset exchange can be mediated by a trusted party or run directly between both parties through a secure off-chain communication channel.

Asset transfer protocols encompass locking, or burning, an asset in the source chain and creating (minting) a representation of that asset in the target chain – *lock-mint* or *burn-mint* pattern, respectively [11]. Once the asset is escrowed in the source chain (by either a centralized party, a multi-signature, or a smart contract), the verification occurs in the target chain. It can be performed by replicating the source chain's consensus mechanism in the target chain [38], [39] or using a proof-based mechanism such as zero-knowledge proofs [40]–[42].

Data Transfers generalize interoperability. Information written in one domain is transferred (or copied) to another accompanied by proof. An example is the payload of a blockchain view [43], where DLT Gateways facilitate the process, running a gateway-to-gateway protocol [44].

2.2. The Source of Truth: Underlying Blockchains

Although the primary focus of this paper is not the security of blockchains, we have to recognize their role as a critical dependency for cross-chain protocols. The reasons are clear: if a transaction t_2 is issued on l_2 based on a rewritten transaction t_1 on l_1, there is a safety violation. For instance, consider a transaction locking an asset in l_1 and a representation minted in l_2. If t_1 reverts, the asset in l_2 becomes unbacked [45]. The probability of this is the same as of a *51% Attack* on the source chain. Proof of Work-based chains subject to forks and Proof of Stake-based chains subject to long-range attacks [46] are some examples of vulnerable chains. Alternatively, chains with instant or near-instant finality, such as those using variants of PBFT [47], do not suffer from the same problem, at the cost of allowing fewer nodes.

2.3. Cross-Chain Events, Transactions and Rules

The concepts of cross-chain events, transactions, and rules are important to understand this work. Transactions issued in one domain trigger internal state changes and emit events based on the operations performed. Cross-chain events are composed of native and non-native domain attributes. Native attributes are retrieved from the events emitted in the underlying domains. Non-native attributes are additional metadata that only hold relevance in cross-chain environments, such as a domain identifier, a global clock, a token price, or other off-chain information. Metadata is published on-chain by decentralized oracles, and its correctness is given by the correctness of the oracle network and according to the agreement between entities to perform $cctxs$.

Definition 1 (Valid Cross-Chain Event)**.** *A cross-chain event e is valid iff its metadata is correct*, and every local transaction $t \in e$ is final.*

The composition of multiple cross-chain events stands for state changes across several domains. We call this composition a cross-chain transaction ($cctx$). To evaluate the validity of a $cctx$, events must be verified against *cross-chain rules* that define the expected behavior. A rule for an asset transfer protocol might indicate that there must not be an event minting an asset in l_2 before an event locking the corresponding asset in l_1. Given some business logic, one can create arbitrarily complex cross-chain rules.

Definition 2 (Valid Cross-Chain Transaction)**.** *A cross-chain transaction $cctx$is valid iff every cross-chain event $e \in cctx$ is valid, and all cross-chain events enforce the defined cross-chain rules.*

3. Cross-Chain Security and Privacy Model

This section presents definitions and formalizes the relevant properties for cross-chain security and privacy. Additionally, it overviews the taxonomy of security- and privacy-enabler approaches for IMs.

3.1. Security Layers

The security of a cross-chain system can be decomposed into the security of several layers. The existing literature supports similar breakdowns [48]. The ***Network Layer*** 🟢 forms the bedrock. It concerns the blockchains that underlie a cross-chain solution (cf. Section 2.2). Above that, the ***Protocol Layer*** 🔵 addresses the different architectural decisions, including defining the actors, their roles, and responsibilities. Further up the stack, we encounter the ***Implementation Layer*** 🟡. It encompasses the entire implementation lifecycle, including off-chain (e.g., relayers, oracles) and on-chain (e.g., smart contracts, protocols) components of the IM. Finally, at the top, the ***Operational Layer*** 🔴 specifies the procedures for deploying, upgrading, operating, and monitoring on- and off-chain components.

3.2. Security Properties

Based on our comprehensive literature review, we propose a set of properties that characterize a secure cross-chain system, inspired by Avizienis et al. [49]. We define

∗. if metadata can be evaluated – e.g., the price of the token being transferred is within an agreed interval

three security properties for IMs: integrity, accountability, and availability.

Definition 3 (Integrity)**.** *Consider an IM and a set of cross-chain rules ζ. Integrity is guaranteed iff every generated $cctx$ respects ζ.*

Definition 4 (Accountability)**.** *An IM is accountable iff these conditions hold: 1) the metadata of any event $e \in cctx$ is public, or at least verifiable†; 2) for every integrity violation attempt in ζ, there is a mechanism to prove it; and 3) there is attempts (e.g., third-party, blockchain smart contract).*

Definition 5 (Availability)**.** *An IM guarantees availability iff it is always able to process (validate, issue, or relay) valid $cctxs$.*

3.3. Security Approaches

The security approaches found in the literature are summarized in Table 1. Interoperability can be facilitated by **Trusted Third Parties** ($\mathcal{SA}_1$) that manage the whole process end-to-end. Alternatively, in **Distributed Trust** ($\mathcal{SA}_2$) approaches, trust is placed on a mechanism run within an external intermediary network. In **Native State Validation** ($\mathcal{SA}_3$) approaches, off-chain parties only relay information to the target chain, and the validity of $cctxs$ is verified on-chain. Finally, **Local Verification** ($\mathcal{SA}_4$) approaches rely on the end users to manually validate each other's transactions on the respective chains. These approaches can be further divided as follows (see table).

3.3.1. ($\mathcal{SA}_{11}$) **Centralization.** Trusted third parties can facilitate interoperability by holding user funds and issuing transactions in $\{l_1, l_2, ..., l_k\}$, or functioning solely as relay services [36], [44]. Trust is placed on the reputation of the managing party [44], [55], [61], [95]. Centralization raises concerns about safety, liveness, and fairness compromises (e.g., bankruptcy, censorship, MEV, money laundering) [59], [62]. On the other hand, it offers greater performance since no agreement between parties is required [50]. Additionally, it enforces accountability as entities must comply with KYC policies [54].

3.3.2. ($\mathcal{SA}_{12}$) **Trusted Computation.** Instead of trusting the reputation of one entity, one can leverage Trusted Execution Environments (TEE) [96] with attestable computation to manage or orchestrate $cctxs$ [21], [60], [61]. TEE-based cross-chain solutions focus on protecting sync committee members' private keys [74], operations on key shares between operators [97], or generate proofs published on multiple chains [74], [98], [99]. Note that attestation keys are still provided by a manufacturer that might, e.g., embed malicious code into the hardware or spoof data [62], [100].

3.3.3. ($\mathcal{SA}_{21}$) **Permissionless Networks.** Compared to decentralized systems, centralized ones are simpler to implement, faster, and cheaper. However, as witnessed multiple times in 2023, they involve security risks [28], [101]–[103]. A solution is to rely on the distribution of power among multiple entities to enforce cross-chain rules and validate $cctxs$ – i.e., through an intermediary distributed network that verifies and maintains proof of actions of other chains [63], [104]–[106]. The security of the IM is driven by the security of the network, both at a technical and financial level, e.g., in PoS-based networks, the overall value protected by the protocol should not exceed the stake held by the majority of validators to avoid protocol deviations [107]. For the same reason, intermediary networks using custom low-value native tokens are not recommended due to fluctuations in token price.

3.3.4. ($\mathcal{SA}_{22}$) **Permissioned Networks.** Instead of relying on a network in which anyone can join, one can opt for a more controlled environment, where validators are whitelisted and, in some cases, are controlled by reputable or trusted entities. These are based on Proof of Authority [108], Threshold Signature Schemes [71], [74] or Multi-Signatures [109]. When parties are not trusted entities, there is usually an identification service deployed, where parties register beforehand [81]. Alternatively, multi-party computation can be used to build trust in environments with mutually untrusted entities [74], [90], [92], [109]. An interesting advantage of $\mathcal{SA}_2$ is to incorporate additional security measures in the intermediary network, such as access control and cross-chain rules enforcement, besides what is in the bridge contracts on the source and destination chains [21], [67].

3.3.5. ($\mathcal{SA}_{31}$) **Inclusion Proofs.** These approaches involve users providing verifiable evidence of actions triggered on one chain on another [38], [77]. Networks of relayers compete to relay block headers (from the source to the destination chain) used to validate user-provided proofs, e.g., Merkle Proofs [38], [69], [110]. Even if a whole network of relayers colluded, they could only disrupt the system if they possess greater mining/voting power than the rest of the source chain, equivalent to mounting a 51% attack on that network. The security of this scheme is based on the security of the light client in the target chain, which depends on the source chain's consensus mechanism. For instance, PoS light clients for the Ethereum 2.0 sync committees ([111]) [39], [40], [76] do not guarantee accountability for the bridge because no slashing mechanism is in place‡.

3.3.6. ($\mathcal{SA}_{32}$) **Validity Proofs.** Validity-proof-based bridges rely on proving systems to validate the state of the source chain's consensus mechanism within the target chain [41], [42], [65], [78], [79]. Unlike $\mathcal{SA}_{31}$, there is no need to understand the consensus logic of other ledgers, as it only requires verifying a succinct zero-knowledge proof (ZKP), which is constant time on zkSNARK-based bridges [112]. Given that circuits are tailor-made to each specific program, the creation of proofs is currently the bottleneck in these

†. for example, private data verifiable through proving systems

‡. https://github.com/ethereum/consensus-specs/issues/3321

TABLE 1. TWO TIER CLASSIFICATION OF SECURITY APPROACHES IN BLOCKCHAIN INTEROPERABILITY ACADEMIC STUDIES. WE PRESENT THE PRIMARY SECURITY APPROACH OF SOLUTIONS THAT EMPLOY VARIOUS.

Security Approach (Tier 1)	Security Approach (Tier 2)	IM Role	References	# (and %)
SA_1 Trusted Third Parties	SA_{11} Centralization	Centralized Services	[21], [36], [50]–[59]	12 (24%)
	SA_{12} Trusted Computation	Trusted Execution Environment	[60]–[62]	3 (06%)
SA_2 Distributed Trust	SA_{21} Permissionless Network	Public Network Validators	[63]–[65]	3 (06%)
	SA_{22} Permissioned Network	Whitelisted Network Validators	[66]–[74]	9 (18%)
SA_3 Native State Verification	SA_{31} Inclusion Proofs	Relayers	[38], [45], [75]–[77]	5 (10%)
	SA_{32} Validity Proofs	Relayers	[41], [42], [78], [79]	4 (08%)
	SA_{33} Fraud Proofs	Relayers	None in academia	0 (00%)
SA_4 Local Verification	SA_{41} Secret- & Time-based Locks	Off-chain Communication Channel	[80]–[94]	15 (29%)

Note: The table categorizes various security approaches (SAs) prevalent in blockchain interoperability research into two tiers. The first tier provides an overarching classification, while the second tier offers a finer granularity. The "IM Role" column denotes the component that takes the role of the Interoperability Mechanism (IM), and the "References" column cites specific studies or implementations that employ the particular approach. The final column quantifies the number and approximate percentage of papers adopting each method, visually represented using cell shading.

systems [40]–[42]. However, new research is improving the efficiency of proof generation, reducing memory demands, and reducing the dependence on trusted setups [105], [113]–[115].

3.3.7. ($\mathcal{SA}_{33}$) **Fraud Proofs.** Fraud proofs provide security for cross-chain protocols by optimistically accepting block headers and other proofs [116]. External watchers can submit fraud proofs to challenge this data [117]. Watchers are rewarded by presenting valid fraud proofs, and operators that sent invalid data see their stake slashed. Transactions based on this information are not final until the fraud-proof period elapses. Usually, to avoid relying on synchronous communication between parties, these periods are extended time windows (∼7 days) [117]. Accountability for relayers is guaranteed. To guarantee safety and liveness, there must be a correct watcher online at all times [118].

3.3.8. ($\mathcal{SA}_{41}$) **Secret-based and time-based locks.** Decentralized atomic swap protocols are commit-reveal schemes based on hash-locks and timelocks [85], or digital signatures [119], [120]. In the former, parties agree on parameters off-chain and have predefined periods in which they must act to complete the protocol. To mitigate atomicity breaches under long-standing crashes, most solutions change the assumptions of synchronous communication by inserting intermediary networks [63], [70], or focus on the usage of *premiums*, a collateralization technique to compensate users in case of misbehavior or crashes [80], [86], [121]. According to [122] collateralization increases the probability that the protocol is completed successfully. There are alternatives to commit-reveal schemes by avoiding the reliance on explicit time intervals. [94] reveals a secret after the counterparty has performed an agreed number of computation steps. The protocol proposed by [91] reveals a full signature once a partial signature is presented. Note that in cross-chain deal [106] and atomic swap protocols [72], [85], [86], [123], [124], safety is usually not defined in terms of atomicity, but rather if honest nodes do not end up worse off than how they started the protocol.

3.4. Privacy Properties

Our survey shows that privacy in cross-chain transactions is a relatively understudied area. In this section, we present the first definition and formalization of generic cross-chain privacy by defining the three most relevant properties: **unlinkability** of *cctxs*, **anonymity** of users and operators, and **confidentiality** of transactional data.

Definition 6 (Cross-Chain Unlinkability)**.** *Consider a cctx between two related accounts $\mathcal{A}_1$ and $\mathcal{A}_2$, where $\mathcal{A}_1$ might be equal to $\mathcal{A}_2$. Transactions t and t' issued by $\mathcal{A}_1$ and $\mathcal{A}_2$, on the source and destination chain, respectively, are said to be unlinked iff an external party cannot infer that t and t' are related to each other.*

External parties can infer relationships between transactions using pre-trained models and heuristics, which return a similarity factor – i.e., the probability of two transactions being linked [125]. Heuristics can be related to transaction amounts, asset profiles [44], reused addresses [126], or transaction patterns [127].

Definition 7 (Cross-Chain Anonymity)**.** *Anonymity of $\mathcal{A}$ holds iff 1) $\mathcal{A}$ cannot be linked to transactions $t_1, ..., t_k$ it has issued in both ledgers and 2) t_i and $t_j, \forall i, j \in [1, k]$ are cross-chain unlinkable.*

Definition 8 (Cross-Chain Confidentiality)**.** *Cross-chain confidentiality holds iff the content of any cross-chain transaction $cctx_1$ issued by an address $\mathcal{A}_1$ is indistinguishable from the content of any other cross-chain transaction $cctx_2$ issued by $\mathcal{A}_1$ or any other address.*

The notion of indistinguishability we are trying to capture is similar to IND-CPA: given two cross-chain transactions $cctx_1$ and $cctx_2$, and their raw payloads p_1 and p_2, respectively, an adversary cannot guess which payload p corresponds to each $cctx$ with a probability higher than 50% (i.e., randomly).

TABLE 2. CLASSIFICATION OF PRIVACY-ENABLER APPROACHES IN BLOCKCHAIN INTEROPERABILITY STUDIES

Privacy Approach	References	# (and %)
PA_1 Zero Knowledge Proofs	[64]–[66], [73], [77]–[79], [81]	8 (47%)
PA_2 Trusted Execution Envir.	[21], [55], [60]	3 (18%)
PA_3 Adaptor Signatures	[87], [92]	2 (12%)
PA_4 Blind Signatures	[93]	1 (06%)
PA_5 Ring Signatures	[74]	1 (06%)
PA_6 Homomorphic Encryption	[88], [89]	2 (12%)

Note: The table categorizes multiple privacy-enabler approaches (PAs) in blockchain interoperability studies. The first column classifies the approach. The second column cites studies or implementations that employ the particular approach. The right-most column estimates the number and percentage of studies adopting each method.

3.5. Privacy-Preserving Approaches

In this section, we overview the main privacy-preserving techniques in the literature, to guarantee at least one of the identified properties. A summary is present in Table 2.

3.5.1. ($\mathcal{PA}_1$) Zero Knowledge Proofs. ZKPs allow proving actions and demonstrate compliance with cross-chain rules without revealing transaction details, involved parties, transaction amounts, or exchange prices [66], [77], [81], [126]. ZKPs are instrumental in validating actions and ensuring compliance with cross-chain rules without disclosing transaction specifics, involved entities, transaction amounts, or exchange rates [66], [77], [81], [126]. These proofs find their applications, e.g., within mixing services. The IM can act as a transaction mixer or leverage existing mixers within the source and destination chains [60], [66], [73].

3.5.2. ($\mathcal{PA}_2$) Trusted Execution Environments. TEEs facilitate computation on private data by preventing data leakage outside the secure enclaves [100]. These promote fairness, for example, in asset exchange protocols with confidential order-matching algorithms [62] (i.e., fairly matching bid and ask orders in exchanges). Due to confidentiality guarantees, the exchange rates are not public, which might help to guarantee unlinkability. TEEs also enable the enforcement of predefined checks to comply with cross-chain rules [21], [62]. A possible approach is to use TEEs as a mixing service [60], but no specific algorithm has been proposed.

3.5.3. ($\mathcal{PA}_3$) Adaptor Signatures. Adaptor signatures allow one party to generate a *pre-signature* on a message associated with a secret, which is guaranteed to provide the secret once the full signature is published [92]. This resembles a commit reveal scheme [87] that underlies HTLCs for asset exchanges. When Party A commits a transaction to collect Party B's assets, it reveals a secret that allows B to redeem A's assets. This protocol avoids publishing the shared secret hash, which makes HTLCs not guarantee unlinkability. It is still possible to analyze on-chain transaction amounts. However, it is unlikely that one can link transactions without knowing the cryptocurrencies exchanged and the exchange rate agreed upon off-chain by both parties.

3.5.4. ($\mathcal{PA}_4$) Blind Signatures. Blind signatures [128] allow users to acquire a signature on a message from a trusted third party without disclosing its specific details. As each blind signature has the same weight, they ensure the unlinkability, anonymity, and confidentiality of cross-chain transactions (even with centralized IMs) [93]. They uphold fairness by shielding against centralized surveillance and eradicating the potential for custom ordering.

3.5.5. ($\mathcal{PA}_5$) Ring Signatures. Ring signatures provide set anonymity by obscuring users among a ring of k users, where the likelihood of exposing an individual's identity is $1/k$ [129]. Notably, revoking anonymity is infeasible, thereby undermining accountability. We acknowledge the existence of different ring signature protocols with trade-offs between, for example, traceability, anonymity, and linkability [130], [131]. The existing literature employs ring signatures to obfuscate sender addresses [109] and protect the identities of intermediary network members, mitigating potential threats such as Denial-of-Service (DoS) attacks [74]. However, due to the inability to identify the signer, in a $cctx$, the transactional data in the source chain must include the destination address, which compromises unlinkability.

3.5.6. ($\mathcal{PA}_6$) Homomorphic Encryption. Similarly to Adaptor Signatures, one can use homomorphic encryption to solve commit-reveal scheme linkability problems. Both [88] and [89] proposed atomic swap solutions based on HE where different secrets are deployed in each chain, attaining transaction unlinkability. Although there are tools for performing basic operations on encrypted data, more research is required to enable more intricate computations and allow general data transfers while guaranteeing confidentiality. Moreover, these protocols typically come with high on-chain computational costs, heavily influenced by the selected homomorphic functions.

4. Status of Cross-Chain Security and Privacy

In this section, we present the results of our work and extensively discuss the most relevant insights. Additionally, we present an extensive list of theoretical cross-chain vulnerabilities, attacks, and mitigations and map them to real-world hacks that account for more than 2.9B USD. We gather all relevant insights and propose guidelines for building secure and robust cross-chain systems.

4.1. Comparison Framework

We classify 51 academic papers and 6 industry solutions in light of the security and privacy models presented in the previous sections, and based on a set of performance and usability metrics relevant to both project maintainers and platform users. Industry solutions are deployed in production, accounting for more than 75% of the TVL in cross-chain bridges [32]. The classification is presented in Table 3.

4.1.1. Classification Criteria. We present the criteria on which we base ourselves to classify the relevant IMs.

TABLE 3. CLASSIFICATION OF BLOCKCHAIN INTEROPERABILITY STUDIES IN ACADEMIA AND INDUSTRY.

				Security			Governance and Performance			Privacy				Misc.		
	Ref	Year	Security Approaches	In	Av	Ac	Dc	Lat	Co	Privacy Approaches	Cf	Un	An	IMode	PC	Impl
Academia	[50]	2019	SA_{11}	◑	○	○	○	◑	◑	–	–	–	–	DT	✓	✓
	[53]	2023	SA_{11}	◑	○	○	●	○	–	–[1]	○	○	○	AT	✓	✗
	[54]	2023	SA_{11}	◑	○	◑	○	○	◑	–[2]	○	○	○	AE	✓	±
	[56]	2023	SA_{11}	◑	○	◑	○	○	◑	–	–	–	–	DT	✓	±
	[58]	2020	SA_{11}	●	○	◑	○	◑	●	–	–	–	–	AE	✓	✓
	[21]	2021	SA_{11}, SA_{12}	○	○	○	○	○	○	PA_2	●	●	–	DT	✗	±
	[57]	2022	SA_{11}, SA_{21}	◑	○	○	◑	–	●	–	◑	○	○	DT	✗	✗
	[51]	2021	SA_{11}, SA_{21}, SA_{22}	◑	◑	○	◑	◑	●	–	–	–	–	DT	✗	✓
	[55][5]	2022	SA_{11}, SA_{22}, SA_{31}	◑	◑	●	○	◑	●	PA_2	◑	○	○	AT	✓	✓[3]
	[36]	2019	SA_{11}, SA_{31}	●	◑	●	◑	◑	–	–[1]	●	●	○	DT	✗	✗
	[52]	2023	SA_{11}, SA_{31}	●	◑	○	○	○	–	–[1]	◑	●	○	AT	✗	±
	[59]	2020	SA_{11}, SA_{41}	◑	◑	○	○	○	–	–	–	–	–	AE	✓	±
	[60]	2021	SA_{12}	◑	○	●	○	○	○	PA_2	●	◑[4]	○	DT	✗	±
	[61]	2021	SA_{12}	◑	○	●	◑	○	○	–	–	–	–	AE	✓	✗
	[62]	2019	SA_{12}	◑	◑	◑	○	○	○	–[2]	○	○	○	AE	✓	±
	[65]	2022	SA_{21}	●	●	○	●	○	○	PA_1	○	◑	◑	DT	✓	±
	[64]	2023	SA_{21}, SA_{32}	●	●	○	●	–	○	PA_1	●	●	●	AE	✗	✓
	[63]	2020	SA_{21}, SA_{41}	●	●	◑	●	◑	●	–	–	–	–	AE	✓	✗
	[67]	2022	SA_{22}	●	●	○	●	–	–	–	–	–	–	AT	✓	✗
	[68]	2019	SA_{22}	●	●	●	◑	○	◑	–	–	–	–	DT	✓	✓
	[71]	2021	SA_{22}	●	◑	○	●	◑	◑	–	–	–	–	DT	✓	✓
	[72]	2021	SA_{22}	◑	◑	○	◑	◑	◑	–	–	–	–	AE	✓	±
	[73]	2023	SA_{22}	●	◑	○	○	◑	○	PA_1	–	●	●	AT	✓	±
	[74]	2022	SA_{22}, SA_{12}	◑	●	●	●	○	○	PA_5	○	○	◑	AT	✓	±
	[69]	2021	SA_{22}, SA_{31}	●	●	◑	◑	○	○	–[1]	●	◑	○	DT	✗	±
	[66]	2023	SA_{22}, SA_{32}	●	●	◑	◑	○	○	PA_1	●	◑	◑	AT	✗	✗
	[70]	2022	SA_{22}, SA_{41}	◑	◑	◑	◑	◑	◑	–	–	–	–	AE	✓	±
	[75]	2022	SA_{31}	●	◑	○	●	◑	–	–	–	–	–	AE	✓	✗
	[76]	2022	SA_{31}	◑	●	○	●	–	◑	–	–	–	–	DT	✓	✓
	[45]	2019	SA_{31}, SA_{21}	◑[6]	●	●	●	◑	◑	–	–	–	–	AT	✓	✓
	[77]	2022	SA_{31}, SA_{21}	◑[6]	○	●	●	◑	○	PA_1	○	●	●	AT	✗	✗
	[38]	2020	SA_{31}, SA_{33}	●	●	◑	●	●	●	–	–	–	–	DT	✓	✓
	[42]	2020	SA_{32}, SA_{22}	●	◑	○	●	○	○	–	–	–	–	DT	✓	✓
	[41]	2022	SA_{32}, SA_{31}	●	◑	○	◑	○	○	–	–	–	–	AT	✓	±
	[78]	2023	SA_{32}, SA_{31}	●	◑	○	●	–	○	PA_1	○	●[7]	●[7]	AT	✓	✓
	[79]	2022	SA_{32}, SA_{31}	●	◑	◑	–	○	○	PA_1	◑	◑	◑	AT	✗	±
	[80]	2021	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	✓
	[81]	2021	SA_{41}	●	◑	●	○	○	○	PA_1	●	●	○	AE	✓	±
	[82]	2022	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	±
	[83]	2022	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	±
	[84]	2021	SA_{41}	●	◑	●	●	◑	●	–	–	–	–	AE	✓	±
	[85]	2018	SA_{41}	●	○	○	●	○	●	–	–	–	–	AE	✓	✗
	[86]	2022	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	✗
	[87]	2020	SA_{41}	●	○	○	●	◑	●	PA_3	●	●	○	AE	✓	✗
	[88]	2022	SA_{41}	●	◑	○	●	◑	●	PA_6	●	◑	○	AE	✓	✗
	[89]	2018	SA_{41}	●	◑	○	●	–	–	PA_6	○	◑	○	AE	✓	✗
	[90]	2022	SA_{41}	●	◑	◑	●	◑	●	–	–	–	–	AE	✓	✓
	[91]	2021	SA_{41}	●	◑	◑	●	◑	●	–	–	–	–	AE	✓	✓
	[92]	2022	SA_{41}	●	◑	◑	◑	◑	●	PA_3	○	◑	○	AE	✓	±
	[93]	2022	SA_{41}	●	○	◑	○	◑	◑	PA_4	○	●	◑	AE	✓	✓
	[94]	2022	SA_{41}	●	●	○	●	◑	●	–	–	–	–	AE	✓	✓
Industry	[132]	2023	SA_{11}, SA_{22}	●	◑	◑	●	◑	●	–	–	–	–	AT	✓	✓
	[133]	2023	SA_{11}, SA_{22}, SA_{33}	●	◑	◑	●	○	●	–	–	–	–	DT	✓	✓
	[134]	2023	SA_{11}, SA_{22}, SA_{33}	●	◑	◑	○	○	●	–	–	–	–	AT	✓	✓
	[135]	2022	SA_{11}, SA_{22}	●	◑	◑	●	◑	●	–	–	–	–	AT	✓	✓
	[136]	2023	SA_{22}, SA_{32}	●	○	◑	○	◑	○	–	–	–	–	DT	✓	±
	[137]	2023	SA_{33}	●	●	◑	●	●	●	–	–	–	–	AT	✓	✓
Metric addressed in paper #(and%)				57(100%)	57(100%)	57(100%)	55(96%)	51(89%)	50(86%)		23(40%)	24(42%)	23(40%)			
Metric guaranteed in paper #(and%)				39(68%)	13(23%)	14(25%)	30(55%)	2(4%)	23(46%)		9(39%)	15(42%)	4(17%)		46(81%)	15(39%)

The classification criteria are in Section 4.1.1. The table identifies the interoperability mode used by each study (**IMode**), indicating whether it supports Asset Transfers (AT), Data Transfers (DT), or Asset Exchanges (AE). Additionally, it notes if the solution is independent of privacy primitives in the underlying chains (**PC**) and if an implementation is available (**Impl**). Papers marked as (–) do not focus on the specific property. The last two rows of the table summarize the classification. We present a visual representation of 1) the number of studies addressing each metric and 2) the number of studies classified using ● or ✓.

Security approaches: SA_{11} Centralization; SA_{12} Trusted Computation; SA_{21} Permissionless Network; SA_{22} Permissioned Network; SA_{31} Inclusion Proofs; SA_{32} Validity Proofs; SA_{33} Fraud Proofs; SA_{41} Secret- & Time-based Locks.

Privacy Approaches: PA_1 ZKP; PA_2 TEE; PA_3 Adaptor Signatures; PA_4 Blind Signatures; PA_5 Ring Signatures; PA_6 Homomorphic Encryption.

[1] Guarantees some privacy properties even if no privacy approach is employed, due to the use of private chains and secure communication channels (e.g., TLS).

[2] Guarantees privacy at the application layer, not the cross-chain level. Protects the order matching protocol to guarantee fairness but transactions are published normally in blockchains.

[3] Has several open-source implementations in different technological stacks, enhancing decentralization.

[4] With considerable liquidity in the TEE [126] we can classify it as ●.

[5] One of the few solutions being standardized in reputable standardization bodies [44].

[6] Strong dependency on price oracle. It can be classified as ● if the oracle is robust and decentralized [7].

[7] Provided it has a sufficiently large anonymity set.

Security Properties.

- *Integrity (In)* Integrity is enforced by the underlying cryptographic primitives which are based on the hardness of well-known problems (e.g., computing the discrete logarithm) (●); integrity is enforced under strong assumptions (e.g., trusted hardware, rational participants, parties abiding by laws) (◑); integrity cannot be guaranteed under misbehaving parties (○).
- *Availability (Av)* Availability requires a decentralized network, but there is at least one honest off-chain party (●); availability can be temporarily compromised if any party misbehaves (◑); it is based on a centralized architecture, hence there are serious concerns about availability (○).
- *Accountability (Ac)* The misbehaving party is identifiable and automatically punished (e.g., programmatically) (●); malicious party is identifiable, but there is no punishment or needs to be enforced by a third party (◑); misbehaving parties are neither identifiable nor punished (○) (the notion of accountable safety [76]).

Privacy Properties.

- *Unlinkability (Un)* It is cryptographically infeasible to link transactions or addresses (●); it is possible to link transactions or addresses through heuristics (◑); no mechanism is in place to unlink transactions or addresses across domains (○).
- *Anonymity (An)* Both users' and operators' identities are concealed (●); users' anonymity or operator's anonymity is enhanced (e.g., through set anonymity approaches) (◑); at most pseudo-anonymity is provided for users, and operators are known (○).
- *Confidentiality (Cf)* Data confidentiality is enforced through cryptographic primitives (●); conditional confidentiality – i.e., can be revoked under some circumstances, or verified by auditors. Note that IMs based on private chains partially guarantee this property (◑); there is no confidentiality (○).

Governance and Performance Properties. We extend our classification of solutions with governance [138] and performance properties, as they are factors that strongly influence security and privacy [8]. We collect insights from related literature to define:

- *Decentralization (Dc)* Fully distributed system with a consensus algorithm to settle different views on information [43] or control relies on the end-user (●); limited decentralization of the system, being run by a small set of verifying parties (◑); control of the system resides in less than 4[§] parties (can be distributed or centralized) (○).
- *Latency (Lat)* Latency of a cross-chain transfer is settled before finalization time (optimistic approach) (●); Latency of a cross-chain transfer is finalized right after the finalization time of the slowest chain (◑); Latency of a cross-chain transfer is more than the finalization time of the slowest chain, due to extra processes ran before (e.g., special account setup) or thereafter (e.g., extra transactions needed) (○).
- *Cost (Co)* there are no protocol fees (for the user); can be run with low-tier commercially available hardware (for IM operator) (●); variable fees depending on search and demand with an upper bound lesser or equal than 1% of the bridged value (for the user); requires at most mid-tier hardware (for IM operator) (◑); variable fees depending on search and demand with more than 1% of the bridged value (for the user); requires above mid-tier and/or specialized hardware for the IM operator (○).

§. some sources suggest that 4 is a reasonable number of non-colluding parties to secure a blockchain bridge [32].

Miscellaneous (Misc.). We provide information that complements our assessment. **IMode** indicates the main interoperability mode supported by the IM. **PC** indicates if the IM requires (✗) a privacy-enhanced chain or permissioned blockchain to operate optimally, or if it is independent of those primitives (✓). **Impl.** refers to the project having an open-source implementation and evaluation (✓), a not-open source implementation (±), or no implementation (✗).

4.1.2. Insights. We now present a list of insights taken from the analysis of the literature.

- **Insight 1:** A conspicuous deficit exists in the literature regarding the empirical assessment of protocol performance and associated costs. This observation is consistent with findings from other studies [8], [139]. While many solutions appear to delegate computationally intensive tasks to off-chain procedures [40]–[42], further investigation in this domain remains paramount.
- **Insight 2:** All studies ensure a degree of integrity, predominantly upheld by cryptographic mechanisms. A thorough examination of these mechanisms is crucial. Research that confines its scope to specific adversarial behaviors (e.g., only rational actors) exhibits diminished integrity.
- **Insight 3:** Security takes precedence over privacy. Only 17 studies (29.8%) address cross-chain privacy. At the same time, projects that dominate 75% of the market neglect cross-chain privacy, suggesting a prevailing apprehension regarding bridge security, relegating privacy to a subordinate design goal.
- **Insight 4:** ZKP ($\mathcal{PA}_1$) emerges as the prevailing approach to guarantee privacy in IMs (53% of IMs with a privacy approach), which allows shifting trust from third parties to cryptographic protocols.
- **Insight 5:** The prevailing academic literature primarily emphasizes asset exchanges (44%) and transfers (29%) between blockchains, with fewer studies addressing general data transfers (26%). This trend contrasts with recent industry developments, with a surge in bridges that facilitate data transfers (arbitrary message-passing bridges, such as [104], [140], [141]).
- **Insight 6:** For cross-chain anonymity, it is imperative that two distinct transactions remain indistinguishable

when originating from the same sender and targeting the same recipient. This condition can only be achieved with the generation of unique addresses for each *cctx*, exemplified by the mechanism of stealth addresses [142].

- **Insight 7:** The predominant trend in the literature underscores the achievement of accountability using stake-slashing mechanisms. In contrast, a smaller subset of research advocates the legal identification of the parties involved through an ancillary identity service. Such methodologies are found predominantly in centralized frameworks within permissioned network configurations where nodes possess identifiable attributes.
- **Insight 8:** Our analysis elucidates that cross-chain unlinkability in AT and DT-based protocols can only be guaranteed when the underlying chains ensure confidentiality. We present a rigorous formalization in Appendix C. For AE protocols, unlinkability can be achieved through cryptographic primitives such as Adaptor Signatures. Additionally, we emphasize the need to investigate heuristics to break privacy [88], [143] and the respective mitigations.
- **Insight 9:** Privacy is implemented with a small set of techniques that bring considerable overhead to IMs, latency- and trust-wise. Both ZKP ($\mathcal{PA}_1$) and TEE ($\mathcal{PA}_2$) require trusted setups with highly expensive computation and specific hardware for achieving confidentiality and unlinkability [21], [126].
- **Insight 10:** Asset exchange protocols, with confidential order matching algorithms [54], [62] do not offer cross-chain privacy. They only guarantee fairness in the order-matching process at the application layer.
- **Insight 11:** Research has shown that the privacy level provided by privacy-centric platforms [144] or applications [145] can be compromised due to risky user behaviors [126], [146]–[149]. Cross-chain systems based on similar primitives face comparable challenges.

4.2. Vulnerabilities, Leaks, and Mitigations

In this section, we present vulnerabilities and leaks found in cross-chain interoperability. Table 4 lists and maps each identified vulnerability/leak to corresponding mitigations. Table 5 presents all mitigations identified in the literature and proposed in this paper.

4.2.1. Vulnerabilities and Leaks. We have identified 45 vulnerabilities across different layers: 3 in the network layer, 22 in the protocol layer, 17 in the implementation layer, and 3 in the operational layer. Many studies focus on common vulnerabilities (e.g., $\mathcal{V}_{13}$, $\mathcal{V}_{18}$ or $\mathcal{V}_{19}$), while specific bug reports highlight more specific issues (e.g., $\mathcal{V}_{14}$ or $\mathcal{V}_{40}$). Surprisingly, we found fewer vulnerabilities in the operational layer, which plays a significant role in cross-chain hacks (cf. Section 4.2.2). Additionally, this might suggest that academia is not addressing industry-relevant issues adequately because the same vulnerabilities are continuously occurring. We have also discovered four theoretical privacy leaks. From our analysis, no privacy leak has been reported in cross-chain systems. Therefore, we could not cross-reference this information with past incidents.

TABLE 4. SECURITY VULNERABILITIES AND PRIVACY LEAKS IN CROSS-CHAIN SYSTEMS. THE COLORED CIRCLE DENOTES THE LAYER WHERE IT CAN BE FOUND (CF. SECTION 3.1).

Vulnerability/Leak	Mitigations
$\mathcal{V}_1$ Honest mining assumption [45]	$\mathcal{M}_1$-$\mathcal{M}_5$
$\mathcal{V}_2$ Absence of identity verification [45], [71], [72]	$\mathcal{M}_8$-$\mathcal{M}_{11}$
$\mathcal{V}_3$ Network isolation [38], [45], [62], [77]	$\mathcal{M}_6$,$\mathcal{M}_7$
$\mathcal{V}_4$ Outdated light client state [45], [53], [150]	$\mathcal{M}_{16}$
$\mathcal{V}_5$ Wrong main chain identification [6], [45], [77]	$\mathcal{M}_{18}$
$\mathcal{V}_6$ Incorrect event verification [151]–[154]	$\mathcal{M}_{12}$-$\mathcal{M}_{14}$
$\mathcal{V}_7$ Acceptance of invalid consensus proofs [155]	$\mathcal{M}_{15}$
$\mathcal{V}_8$ Absence of chain identification [156]	$\mathcal{M}_4$
$\mathcal{V}_9$ Submission of repeated inclusion proofs [21], [45], [77], [157]	$\mathcal{M}_{17}$
$\mathcal{V}_{10}$ Counterfeiting assets [45], [77], [158]	$\mathcal{M}_{19}$-$\mathcal{M}_{23}$
$\mathcal{V}_{11}$ Involuntary timelock expiry [63], [85]	$\mathcal{M}_{29}$-$\mathcal{M}_{30}$
$\mathcal{V}_{12}$ Unset withdrawal limits [156], [159]	$\mathcal{M}_{69}$
$\mathcal{V}_{13}$ Action withhold [58], [61], [80], [86], [86], [94], [160]	$\mathcal{M}_8$,$\mathcal{M}_{27}$,$\mathcal{M}_{28}$
$\mathcal{V}_{14}$ Unspecified gas limit [161]	$\mathcal{M}_{65}$
$\mathcal{V}_{15}$ Resource exhaustion [45], [55], [57], [60], [65], [69]	$\mathcal{M}_{48}$-$\mathcal{M}_{50}$
$\mathcal{V}_{16}$ Single point of failure [156], [162]	$\mathcal{M}_7$,$\mathcal{M}_{32}$,$\mathcal{M}_{47}$
$\mathcal{V}_{17}$ Publicly identifiable operators [74]	$\mathcal{M}_{44}$-$\mathcal{M}_{46}$
$\mathcal{V}_{18}$ Misaligned incentive mechanisms [38], [60], [65], [122]	$\mathcal{M}_{23}$,$\mathcal{M}_{31}$-$\mathcal{M}_{34}$
$\mathcal{V}_{19}$ Token price volatility [45], [74], [77], [80], [82], [83]	$\mathcal{M}_{35}$-$\mathcal{M}_{39}$
$\mathcal{V}_{20}$ Centralized power [65], [162], [163]	$\mathcal{M}_{32}$,$\mathcal{M}_{43}$
$\mathcal{V}_{21}$ Verifier's dilemma [163]	$\mathcal{M}_{24}$-$\mathcal{M}_{26}$
$\mathcal{V}_{22}$ Manipulation of exchange rates [29], [164]–[167]	$\mathcal{M}_{40}$,$\mathcal{M}_{41}$
$\mathcal{V}_{23}$ Unfair transaction/event ordering [65]	$\mathcal{M}_{41}$,$\mathcal{M}_{42}$
$\mathcal{V}_{24}$ Insecure access control [168]–[173]	$\mathcal{M}_{51}$,$\mathcal{M}_{52}$
$\mathcal{V}_{25}$ Conceed approvals to third parties [152], [174], [175]	$\mathcal{M}_{53}$
$\mathcal{V}_{26}$ Outdated third-party library version [176]	$\mathcal{M}_{78}$
$\mathcal{V}_{27}$ Unsafe third party modules [151], [156], [162], [177]	$\mathcal{M}_{58}$,$\mathcal{M}_{78}$
$\mathcal{V}_{28}$ Dead code [151], [159], [176]–[180]	$\mathcal{M}_{59}$
$\mathcal{V}_{29}$ Usage of non-standard naming [176], [177]	$\mathcal{M}_{79}$
$\mathcal{V}_{30}$ Inconsistent smart contract engine version [156], [162], [179]	$\mathcal{M}_{80}$
$\mathcal{V}_{31}$ Unconventional code/testing architecture [176], [179]	$\mathcal{M}_{81}$
$\mathcal{V}_{32}$ Reentrancy [156]	$\mathcal{M}_{82}$
$\mathcal{V}_{33}$ Failure to emit events upon state changes [151], [162], [178]	$\mathcal{M}_{83}$
$\mathcal{V}_{34}$ Inconsistent bridge contract interfaces [180]	$\mathcal{M}_{84}$
$\mathcal{V}_{35}$ Out of order transaction execution [151]	$\mathcal{M}_{85}$
$\mathcal{V}_{36}$ Absence of storage gaps in smart contracts [181]	$\mathcal{M}_{86}$
$\mathcal{V}_{37}$ Integer overflow and underflow [151], [159], [162], [176]	$\mathcal{M}_{87}$
$\mathcal{V}_{38}$ Absence of sanity checks [156], [177]	$\mathcal{M}_{87}$
$\mathcal{V}_{39}$ Code and documentation mismatched [162], [176]–[179]	$\mathcal{M}_{88}$
$\mathcal{V}_{40}$ Uninitialized variables [182]	$\mathcal{M}_{66}$
$\mathcal{V}_{41}$ Compromise of ZK algorithms' private inputs [126]	$\mathcal{M}_{67}$
$\mathcal{V}_{42}$ Other smart contract vulnerabilities [151], [162], [179]	$\mathcal{M}_{51}$,$\mathcal{M}_{54}$-$\mathcal{M}_{56}$
$\mathcal{V}_{43}$ Inadequate key management [152], [183]	$\mathcal{M}_{47}$,$\mathcal{M}_{60}$-$\mathcal{M}_{62}$
$\mathcal{V}_{44}$ Physical infrastructure backdoors [50]	$\mathcal{M}_{46}$,$\mathcal{M}_{63}$-$\mathcal{M}_{64}$
$\mathcal{V}_{45}$ Social engineering-related vulnerabilities [174], [184]	$\mathcal{M}_{77}$
– $\mathcal{L}_1$ Leakage of private data in ZK ceremony input [40]	$\mathcal{M}_{89}$
– $\mathcal{L}_2$ Linking transactions through transactional data [88], [89]	$\mathcal{M}_{90}$
– $\mathcal{L}_3$ Common secret deployment [87]	$\mathcal{M}_{91}$
– $\mathcal{L}_4$ User-generated privacy leaks [126], [146]–[149]	$\mathcal{M}_{92}$
– $\mathcal{L}_5$ Mapping on-chain addresses to real-world identities [126]	$\mathcal{M}_{90}$, $\mathcal{M}_{92}$

4.2.2. Analysis of Real-World Hacks. Attacks against cross-chain bridges have proliferated in the last couple of years. Table 6 presents a classification of 14 of the most impactful attacks in the industry since July 2021, that account for more than 94% of the total value stolen from cross-chain bridges. We present general attack information, incident response-related data, the components targeted by attackers, and the vulnerabilities behind each. Appendix E presents further information and mitigations for each.

Security Approach (SA) The security approach used by the bridge.

TABLE 5. LIST OF MITIGATIONS COLLECTED IN THE LITERATURE AND PROPOSED BY OUR ANALYSIS

Label	Ref	Mitigation description
$\mathcal{M}_1$	[75]	Wait full confirmation time according to the source chain consensus mechanism
$\mathcal{M}_2$	[45]	Insertion of block maturity periods
$\mathcal{M}_3$	[43]	Usage of blockchain views
$\mathcal{M}_4$	[156]	Add chain identification mechanisms
$\mathcal{M}_5$	[45]	Synchronize smart contract state on multiple destination chains
$\mathcal{M}_6$	[38]	Increase transaction settlement time
$\mathcal{M}_7$	[50]	Physical decentralization of infrastructure
$\mathcal{M}_8$	[54]	Usage of a trusted centralized authority to mediate *cctxs*
$\mathcal{M}_9$	[185]	Integration with Self Sovereign Identity (SSI) mechanisms
$\mathcal{M}_{10}$	[72]	Make the creation of identities expensive (e.g., a high stake per identity)
$\mathcal{M}_{11}$	[71]	Reward creating fewer identities with more stake
$\mathcal{M}_{12}$	[152]	Listen to events only from whitelisted smart contracts
$\mathcal{M}_{13}$	[154]	Deploy runtime monitoring modules
$\mathcal{M}_{14}$	[65]	Employ multiple different monitoring strategies at the same time
$\mathcal{M}_{15}$	[76]	Enable verifiability of state updates in light clients for different consensus mechanism
$\mathcal{M}_{16}$	[150]	Insertion of a data availability layer
$\mathcal{M}_{17}$	[77]	Unique nonce/id generation per request
$\mathcal{M}_{18}$	[45]	Use and develop new main chain identification mechanisms
$\mathcal{M}_{19}$	[77]	Trigger automatic liquidations of collateral
$\mathcal{M}_{20}$	[45]	Use Collateralization / Over-Collateralization techniques
$\mathcal{M}_{21}$	[117]	Usage of external incentivized watchers that attest actions/events
$\mathcal{M}_{22}$	[141]	Embedded rules in third party network consensus mechanism
$\mathcal{M}_{23}$	[90]	Usage of Distributed Signature Schemes between untrusted users and operators
$\mathcal{M}_{24}$	[163]	Parallelizing transaction verification
$\mathcal{M}_{25}$	–	Insert independent computational-heavy transactions into multiple blocks
$\mathcal{M}_{26}$	[186]	Separate entities that create and verify blocks
$\mathcal{M}_{27}$	[80]	Usage of Premiums
$\mathcal{M}_{28}$	[186]	Usage of Verifiable Timed Commitments
$\mathcal{M}_{29}$	[63]	Provide support for periods of asynchrony in the execution of the protocol
$\mathcal{M}_{30}$	[91]	Use pre-deployed refund transactions/contracts triggered upon failures
$\mathcal{M}_{31}$	[122]	Model and analyze user behaviour through game-theory principles
$\mathcal{M}_{32}$	[187]	Protocol architecture decentralization
$\mathcal{M}_{33}$	[38]	Increase the number of parties and scatter mining power among them
$\mathcal{M}_{34}$	[84]	Usage of MEV to front-run misbehaving transactions
$\mathcal{M}_{35}$	[82]	Parallel asset locking
$\mathcal{M}_{36}$	[82]	Reduce time window for users to observe price fluctuations
$\mathcal{M}_{37}$	[45]	Over-collateralization to account for slippage
$\mathcal{M}_{38}$	[45]	Adjust the amount locked according to the updated exchange rates
$\mathcal{M}_{39}$	[45]	Trigger automatic liquidations to avoid getting uncollateralized
$\mathcal{M}_{40}$	[187]	Merge multiple sources of data
$\mathcal{M}_{41}$	[188]	General mitigations for (MEV), such as confidential mempools
$\mathcal{M}_{42}$	[189]	Enforce predefined transaction ordering rules
$\mathcal{M}_{43}$	[163]	Overlap capabilities between multiple parties
$\mathcal{M}_{44}$	[74]	Employ evolving committees rather than static ones
$\mathcal{M}_{45}$	[184]	Hide one public key among multiple keys of other users/operators
$\mathcal{M}_{46}$	[50]	Other usual web2 infrastructure backdoor mitigations
$\mathcal{M}_{47}$	[50]	Decentralization at the operational level (e.g., key management and monitoring)
$\mathcal{M}_{49}$	[36]	Use redundant nodes or deploy logic in the blockchain (i.e., in smart contracts)
$\mathcal{M}_{50}$	[50]	Usual web2 practices (e.g., rate limiting, challenge-response tests)
$\mathcal{M}_{51}$	–	Multiple rounds of smart contract audits, preferably by different parties
$\mathcal{M}_{52}$	[44]	Standardization of cross-chain bridge design (e.g., for proper access control)
$\mathcal{M}_{53}$	[175]	Do not issue approvals for more funds than what is strictly necessary
$\mathcal{M}_{54}$	[190]	General smart contract vulnerabilities mitigations
$\mathcal{M}_{55}$	–	Submit codebases to thorough code reviews before production
$\mathcal{M}_{56}$	–	Ensure there are rigorous testing guidelines being enforced
$\mathcal{M}_{57}$	–	Just like on-chain smart contracts, off-chain programs and infrastructure must be audited
$\mathcal{M}_{58}$	[162]	Avoid library version auto-upgrades and audit code before upgrading
$\mathcal{M}_{59}$	–	Linting tools to raise warnings for unused code
$\mathcal{M}_{60}$	[191]	Improve cryptographic key management (e.g., usage of hardware or cold wallets)
$\mathcal{M}_{61}$	[60]	Increase of the number of validators and thresholds in multi-signature wallets
$\mathcal{M}_{62}$	[50]	Employ further authentication mechanisms to protect keys
$\mathcal{M}_{63}$	[50]	Accept incoming connections only from whitelisted IP addresses
$\mathcal{M}_{64}$	[50]	Authenticate requests made to RPC nodes through rotating keys
$\mathcal{M}_{65}$	[161]	Require setting gas limits for *cctxs*
$\mathcal{M}_{66}$	–	Performe deep optimizations once the industry and the project have reached stability
$\mathcal{M}_{67}$	[40]	Dispose of private inputs used to generate the CRS in zk-based solutions
$\mathcal{M}_{68}$	[153]	Monitor on- and off-chain infrastructure
$\mathcal{M}_{69}$	[141]	Set appropriate withdrawal limits and implement a freezing functionality
$\mathcal{M}_{70}$	[175]	Do not give excessive permissions to individual external entities
$\mathcal{M}_{71}$	[172]	Check inputs in arbitrary message passing bridges for function signatures' hash collision
$\mathcal{M}_{72}$	–	Treat critical fixes internally before pushing them to public repositories
$\mathcal{M}_{73}$	–	Make sure critical components are updated before an audit, not afterwards
$\mathcal{M}_{74}$	–	Do not launch projects on top of existing ones without knowing the inner details
$\mathcal{M}_{75}$	–	Fix bugs as soon as they are detected, not just leaving for the future
$\mathcal{M}_{76}$	[8]	Follow standard practices, such as RFCs.
$\mathcal{M}_{77}$	–	Increasing the awareness of all involved actors
$\mathcal{M}_{78}$	[176]	Attest the security of external packages using analysis tools and third-party auditors
$\mathcal{M}_{79}$	[179]	Follow coding practices according to the programming language being used
$\mathcal{M}_{80}$	[162]	Apply the same (or compatible) compiler version across the whole project
$\mathcal{M}_{81}$	[177]	Follow standard code/testing architectures to prioritize understandability of the code
$\mathcal{M}_{82}$	[156]	Update the internal state of a contract before making an external call to another one
$\mathcal{M}_{83}$	[162]	Document critical state changes and – e.g., one event should be emitted for each one
$\mathcal{M}_{84}$	[180]	Reuse code for the definition of messages for components that interact with one another
$\mathcal{M}_{85}$	[151]	Enforce transaction ordering between L1s and L2s
$\mathcal{M}_{86}$	[156]	Follow standards for the usage of storage gaps within upgradeable smart contracts
$\mathcal{M}_{87}$	[192]	Use (e.g., static) analysis tools to warn the absence of checks on inputs and operations
$\mathcal{M}_{88}$	[178]	Force documentation and comments to be updated once pull requests are accepted
$\mathcal{M}_{89}$	–	Providing a user-agnostic and random string as input for the ZK trusted ceremony phase
$\mathcal{M}_{90}$	[144]	Use unique addresses – e.g., using primitives such as stealth addresses
$\mathcal{M}_{91}$	–	Rely on alternative atomic-reveal schemes – e.g., Diffie Hellman and Adaptor Signatures
$\mathcal{M}_{92}$	[146]	Educate users for privacy-preserving practices – e.g., address reuse and unique gas prices

Note: The table displays various security and privacy vulnerability mitigations. We have included references to indicate the source of each vulnerability and marked our proposals with "–".

Date The date of the first transaction exploiting a vulnerability in the protocol.

Amount The amount in USD stolen from the cross-chain bridge. We do not include any collateral losses in other protocols.

Attacker Type (AT) We classify attackers as black or white hats based on whether they returned the funds (or both if there is at least one attacker of each type). Attackers who returned the funds, excluding agreed bounty fees, are also considered white hats in our analysis.

Number of Transactions (Txs) A range of the number of transactions issued by the attackers to exploit the bridge, including both external and internal transactions, which are transactions issued directly by the user or as a consequence of another contract execution, respectively. It does not include transactions issued before or after the attack to exchange or launder funds using DEXes (e.g., Uniswap) or mixing services.

Usage of Mixers (Mix) The usage of transaction mixers (e.g., Tornado Cash) by the attacker to launder funds either before or after attacks to break the linkability of transactions.

Discovery Time (DT) The time it took maintainers to discover the attack and trigger the corresponding incident response mechanism. Given that this information is internal to each team, we contacted each of the 14 projects and asked them to provide us with data.

Communication Time (CT) The time it took maintainers to communicate the exploit to the community. This communication was performed solely as *Tweets*. This value is the difference between the timestamp of the *Tweet* and the timestamp of the first exploit transaction.

Vulnerability Location (VL) We identify the location of each vulnerability: in the *Source Chain Smart Contract* – the component with the bridging logic in the source chain, responsible for escrowing funds; in the *Target Chain Smart Contract* – the element with the bridging logic in the source chain, responsible for verifying inclusion proofs; or in the *Interoperability Mechanism* – the off-chain component that enables interoperability, usually composed of validators/relayers.

Exploit Location (EL) A vulnerability in one location can originate exploits in others. We classify the location of the exploit as follows: in the *Source Chain Smart Contract* if the attacker stole escrowed funds; in the *Target Chain Smart Contract* if the attacker minted unbacked funds; or in the *Business Logic Smart Contract* if the attacker stole funds by exploiting the business logic contract – usually because users approved a bridge-controlled contract to manage their funds (e.g., through the *approve()* function in the ERC20 token standard).

4.2.3. Insights. We present a list of insights taken from the analysis of cross-chain bridge hacks.

- **Insight 1:** 65.8% of the total value stolen originated in bridges based on intermediary permissioned networks (SA_{22}). Projects choose SA_{22} to have finer control over the bridge. However, it also eases hackers' efforts to gain control over the infrastructure. Three hacks were performed on both solutions that rely on centralized services (SA_{11}) and intermediary permissionless networks (SA_{21}) (26.8% and 0.5% of the total value, respectively); and two projects based on fraud proofs (SA_{33}) (6.9%). IMs based on Local Verification (SA_4) do not enter the leaderboard.
- **Insight 2:** Limiting the number of internal transactions within the same contract or the amount moved per external transaction is possible and advisable. We believe setting withdrawal limits or emergency pauses would significantly reduce this value. Even though this does not avoid an attack, it serves as a cornerstone step in the first phases of incident response.
- **Insight 3:** Only one hack is classified as being performed by a white hat, as almost all funds were returned. Moreover, only around 35M USD were returned (1.5% of the hacked amount). There is clearly a lack of motivation for hackers to disclose vulnerabilities. There is little transparency concerning the bounties offered [205].
- **Insight 4:** Notably, in 14 of the hacks authored by black hats, transaction mixers were used 5 times before the attack (35.7%) and 11 times after the attack (78.6%). The pNetwork hackers did not use any mixer and still retain the funds in their accounts [206]. In the PolyBridge #1 hack, the hacker returned a noteworthy portion of 611M USD after negotiations [207]. We believe these cases highlight the difficulty of money laundering in blockchain environments due to the inherent traceability of blockchain transactions [208].
- **Insight 5:** We find that the *lock-mint* model for asset transfer bridges is riskier than other approaches. Attackers target escrowed funds in the source chain. Eight hacks drained funds from the escrow in the source chain, accounting for 1.8B USD (62%). Using native tokens instead of wrapped assets is a solution that allows developers to implement one-way flows – *burn-mint* models. An example is Circle's USDC announcement in October 2023. USDC is now burned in Ethereum and minted natively on Polygon [209].
- **Insight 6:** Two teams took 5 and 13 minutes to detect the incidents. The Ronin bridge team took 6 days. This information emphasizes the need for improvement in incident detection for swift attack detection. Work has been done designing cross-chain models to identify and visualize deviations from expected behavior [153], [154], [210].

4.3. Recommendations to Cross-Chain Bridge Operators

We divide the different guidelines for cross-chain systems into three different domains.

4.3.1. Implementation Layer. Due to the ad-hoc design and implementation of cross-chain projects [177], [211], attacks exploiting well-known vulnerabilities are still surfacing [212]. Smart contracts, just like any software com-

TABLE 6. CLASSIFICATION OF MOST PROFITABLE CROSS-CHAIN BRIDGE HACKS GROUPED BY SECURITY APPROACH. THE AMOUNTS ARE PRESENTED IN USD. THE CELLS WITH THE VULNERABILITY NUMBER ARE FILLED WITH THE COLOR ACCORDING TO THE LAYER THEY BELONG TO (CF. SECTION 3.1). WE ADD A "SUMMARY" ROW THAT AGGREGATES INFORMATION. SPECIFICALLY, WE USE CELL SHADING TO SHOW THE PERCENTAGE OF HACKS IN WHICH EACH VULNERABILITY WAS FOUND.

Project Information		General Attack Information					Incident Resp		Where		Mapping to Theoretical Vulnerabilities					
Name & Ref	SA	Date	Amount	AT	Txs	Mix	DT	CT	VL	EL	$\mathcal{V}_{44}$	$\mathcal{V}_{43}$	$\mathcal{V}_{28}$	$\mathcal{V}_{27}$	$\mathcal{V}_{24}$	$\mathcal{V}_{6}$
[193] Ronin	$\mathcal{SA}_{22}$	Mar 2022	624M	■	○	◑	6d	●	IM	SC	✓	✓	✗	✗	✗	✗
[194] PolyBridge #1	$\mathcal{SA}_{22}$	Aug 2021	611M	□	◔	○	–	◔	TC	SC	✗	✓	✓	✗	✗	✗
[195] BNB	$\mathcal{SA}_{11}$	Oct 2022	566M	■	◔	◐	–	◑	TC	TC	✗	✗	✗	✗	✓	✗
[108] Wormhole	$\mathcal{SA}_{22}$	Feb 2022	326M	■	○	◐	–	○	TC	TC	✗	✗	✓	✗	✓	✗
[196] Nomad	$\mathcal{SA}_{33}$	Aug 2022	190M	◧	◕	◑	–	◔	SC	SC	✗	✗	✗	✗	✓	✗
[197] BXH	$\mathcal{SA}_{11}$	Oct 2021	139M	■	○	◐	–	◑	–	SC	✓	✓	✗	✗	✗	✗
[198] Multichain #2	$\mathcal{SA}_{22}$	Jul 2023	126M	■	○	○	–	◑	IM	SC	✓†	✓†	✗	✗	✗	✗
[199] Harmony	$\mathcal{SA}_{22}$	Jun 2022	100M	■	◔	◑	–	◕	IM	SC	✓	✓	✗	✗	✗	✗
[200] Qubit	$\mathcal{SA}_{11}$	Jan 2022	80M	■	◔	◑	–	◔	SC	TC	✗	✗	✗	✓	✓	✗
[201] pNetwork	$\mathcal{SA}_{33}$	Sep 2021	13M	■	◔	○	13m	◔	IM	SC	✗	✗	✗	✗	✗	✓
[202] Thorchain #3	$\mathcal{SA}_{21}$	Jul 2021	8M	■	○	◑	–	–	IM	SC	✗	✗	✗	✗	✗	✓
[198] Anyswap	$\mathcal{SA}_{22}$	Jul 2021	8M	■	○	◑	–	◕	IM	TC	✗	✓	✗	✗	✗	✗
[202] Thorchain #2	$\mathcal{SA}_{21}$	Jul 2021	5M	■	◕	◑	–	◑	IM	TC	✗	✗	✗	✗	✓	✓
[194] PolyBridge #2	$\mathcal{SA}_{22}$	Jul 2023	4.4M	■	◑	○	7h	◕	IM	TC	✗	✓	✗	✗	✗	✗
[203] Meter	$\mathcal{SA}_{22}$	Jul 2021	4.4M	■	○	◑	–	◔	SC	TC	✗	✗	✗	✗	✓	✗
[204] Chainswap	$\mathcal{SA}_{22}$	Jul 2021	4.4M	■	●	●	–	◑	TC	TC	✗	✗	✓	✗	✓	✗
[198] Multichain #1	$\mathcal{SA}_{22}$	Jan 2022	3M	◧	–	●	–	◕	TC	BL	✗	✗	✗	✓	✓	✗
[202] Thorchain #1	$\mathcal{SA}_{21}$	Jun 2021	140K	■	–	◑	5m	–	IM	TC	✗	✗	✗	✗	✗	✓
Summary		**07/21 - 07/23**	**2.9B**								**22%**	**39%**	**17%**	**11%**	**44%**	**22%**

Attacker Type (AT)
■ Black hat
□ White hat
◧ Black and white hats

Number of Transactions (Txs)
○ 1-10
◔ 10-50
◑ 50-100
◕ 100-1000
● >1000

Usage of Mixers (Mix)
○ Not used
◐ Before the attack
◑ After the attack
● Before and after the attack

Communication Time (CT)
○]0; 2] hours
◔]2; 4] hours
◑]4; 6] hours
◕]6; 24] hours
● >= 6 days

Vulnerability/Exploit Location (VL/EL)
SC Source Chain SC
TC Target Chain SC
IM Interoperability Mechanism
BL Business Logic SC

– No information available / Team did not respond

† Still to be confirmed

Discovery Time (DT)

ponent, are vulnerable to attacks [33], [190], [213], [214]. To address these vulnerabilities, developers must implement secure coding practices, use continuous integration [215], propose design patterns, and use tools to identify and mitigate potential security issues in the codebase. These include static analysis (e.g., Slither [192], Mythril [216], Mythx [217]), formal verification [218], fuzz testing (e.g., Echidna [219], Harvey [220]), vulnerability detection at runtime (e.g., Scribble [221]), and more recently AI tools to identify vulnerable patterns and perform analysis of control/data flow graphs [33]. It is essential that these tools focus on the composability of smart contracts and not just on the analysis of isolated components.

4.3.2. Protocol Layer. Decentralization is paramount for cross-chain solutions, as is evident in Table 6. An infrastructure breach or key compromise can prove catastrophic for platforms that manage substantial funds. For solutions rooted in permissioned networks, it is vital to emphasize due diligence in selecting parties and ensuring expected validator performance, protocol involvement, and compliance with Service Level Agreements (SLA) [107]. Although this approach places greater responsibility on users, a viable mitigation strategy to minimize the likelihood of incidents involves increasing the reliance on user- and Dapp-specific inputs directly submitted to the target chain [65].

We highlight some practices that are of critical importance. On-chain authentication and proof verification mechanisms must be carefully designed and audited by multiple entities. Access control to contracts with critical functionality must be guaranteed by a studied cross-chain model and architecture. Additionally, our recommendations include the usage of formal frameworks to prove the correctness of protocols (e.g., UC [222] or TLA+ [223]), game-theoretical analysis of incentivization, and slashing mechanisms.

4.3.3. Operational Layer. At the forefront of originating cross-chain hacks is inadequate key management (1.6B USD stolen, 55%). Although solutions like Hardware Security Modules (HSM) and hardware wallets exist, their scope is limited. To mitigate risk, implementing secure protocols for rotating validator keys could limit the potential for single points of failure. Daily withdrawal limits also emerge as a practical measure to reduce losses during an attack. Table 6 indicates that hackers prefer exploiting vulnerabilities over disclosing them. Therefore, attractive bug bounty programs serve as a compelling avenue to incentivize ethical hackers to report vulnerabilities in open-source code. However, open-source software can expose internal mechanisms and potential security flaws, which has happened twice (cf. Table 10). We, therefore, highlight the need for developers to strike a delicate balance between transparency, collaboration, and system protection. We advocate for multiple accredited entities to verify smart contracts and conduct risk assessments [32].

4.4. Future Research Directions

Our research has identified several areas within the blockchain community that require further exploration and

development. Firstly, there is a need for proactive prevention through continuous monitoring of all components, which is not yet a structured practice. Secondly, there is a lack of comprehensive incident response frameworks for generic cross-chain systems despite some industry-specific endeavors. Additionally, the community must focus on designing new techniques to ensure unlinkability and anonymity across diverse ledgers. Furthermore, there is a need to conduct a comprehensive study of design patterns across interoperable blockchain systems. Notably, strides have been made towards a universal data model through the ISO model adopted by Overledger [224], SATP Gateways [44], and IBC [225]. However, the path to standardization is still being explored, with multiple emerging standards. Finally, there is a significant gap in empirical studies addressing the detection of theoretical attacks and associated mitigation strategies identified in our analysis, such as cross-chain Miner Extractable Value (MEV) and oracle manipulation [65], [226]. Appendix D presents some additional considerations.

4.5. Summary

The importance of comprehensive security in cross-chain operations cannot be understated. Despite extensive research conducted on cross-chain security, ensuring protection across the entire stack remains imperative. Given the vast attack surface, relying solely on preventive measures, such as continuous monitoring and proactive security, does not suffice. We strongly recommend that practitioners bolster their defenses by integrating reactive security measures, including robust incident response frameworks.

Concerning privacy, current research appears to be relatively underexplored. However, as interoperable central bank digital currencies gain traction [95], [227], we foresee a more substantial impetus driving advances in cross-chain privacy solutions. Full unlinkability in a permissionless cross-chain scenario is hard to achieve since at least one entity needs to perform the mapping between transactions on both the source and destination chains. We envision that protocols that fill this gap will emerge, especially with the recent evolution of zero-knowledge technology. In practice, transaction mixers do not yield a high degree of privacy to users due to their naive practices. Solutions circumventing these limitations are necessary. Furthermore, existing mixers are being used for malicious activities. Therefore, we highlight the importance of researching how to guarantee privacy in regulated and auditable environments.

5. Related Work

We compare blockchain security and privacy studies with our work in Table 7. Our study stands out by 1) employing a systematic survey grounded in recognized principles, 2) fusing essential security and privacy dimensions, and 3) encompassing findings from gray literature and the industry for comprehensive scrutiny, offering developers practical insights to enhance system robustness and privacy. In recent years, notable surveys have emerged[3], [7], [11], [228]. Our examination of security and privacy intricacies revolves around cross-chain rules, explored through various methodologies such as runtime verification [229], formal definitions upheld by off-chain relayers and smart contracts [153], and other formulations to detect discrepancies in bridge mechanisms [154]. Some studies implicitly address cross-chain rules, while others explicitly define them in discussions on oracles [230], [231], bridges [116], and gateways [44].

TABLE 7. COMPARISON OF THIS PAPER WITH OTHERS ON SECURITY OR PRIVACY OF BLOCKCHAIN INTEROPERABILITY. *All labels apply to systematizations.*

	Security				Privacy				Misc.	
Ref	P	V	A	M	P	V	A	M	R	IM
[17]	✗	✓[15]	✓[1]	✓[18]	✗	✓[1]	✗	✓[1]	46	2
[13]	✗	✓[29]	✓[7]	✓[13]	✗	✓[1]	✗	✗	–	6
[232]	✗	✗	✗	✗	✓	✗	✗	✓[4]	–	29
[233]	✗	✓[11]	✓[18]	✓[6]	✗	✗	✗	✗	–	–
this work	✓	✓[45]	✓[18]	✓[92]	✓	✓[5]	✗	✓[3]	212	57

✓ – Satisfies criteria
✗ – Does not satisfy criteria
P – Identifies relevant properties
A – Real-World attacks or leakages
M – Identifies or proposes mitigations
R – Number of relevant references
V – Identifies cross-chain vulnerabilities
IM – Number of interoperability mechanisms systematically studied
– Not specified by the authors

Since blockchain's inception, security has been a key research focus [234]. Studies have aimed to formalize security properties [235]–[240] and consolidate this knowledge across various layers, such as network, protocol, and operations [241]–[246]. Research has extensively delved into attacks in the same layers [234], [244], [247]–[249]. Our exploration of privacy builds on seminal work on anonymity, unlinkability, and confidentiality [125], [250]. Although there are endeavors to introduce permissioned and privacy-oriented blockchains [251], [252], privacy research in interoperability primarily focuses on asset exchanges. Our conceptual model is based on [87] and extends to cover all interoperability modes.

6. Conclusion

This paper systematizes the relevant security and privacy properties and approaches in blockchain interoperability research. We correlate theoretical vulnerabilities and 14 cross-chain bridge hacks, collectively responsible for 94% of the total hacked value up to date. Our data shows that security is a more pressing concern than privacy and that permissioned intermediary networks are the most vulnerable security approach. Regarding privacy, our survey reveals a prevalent reliance on zero-knowledge technology. Although this method is promising, it requires extensive additional research before being widely adopted. We collect and propose mitigations for identified vulnerabilities and outline various research pathways, such as reliable monitoring of IMs, incident response frameworks, the need for empirical studies, and further exploration of cross-chain privacy.

Acknowledgments

We thank Dave Pasirstein and our colleagues in the IETF's SATP working group for fruitful discussions. We appreciate the DPSS group at INESC-ID for suggestions and discussion on this paper. Rafael thanks the Fulbright Association, Thomas Hardjono, and Alex Pentland for the opportunity to research at the MIT Media Lab, where this work was partially developed. We thank Guy Zyskind and colleagues from the MIT Media Lab for fruitful discussions on blockchain privacy and interoperability. Rafael was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020 (INESC-ID) and 2020.06837.BD, and a research scholarship from the Fulbright Association, with the support of FCT. This work was developed within the scope of the project nr. 51 "BLOCKCHAIN.PT - Agenda Descentralizar Portugal com Blockchain", financed by European Funds, namely "Recovery and Resilience Plan - Component 5: Agendas Mobilizadoras para a Inovação Empresarial", included in the NextGenerationEU funding program. Luyao Zhang is supported by the National Science Foundation China on the project entitled "Trust Mechanism Design on Blockchain: An Interdisciplinary Approach of Game Theory, Reinforcement Learning, and Human-AI Interactions (Grant No. 12201266)." Luyao Zhang is also with SciEcon CIC, a not-for-profit (NPO) organization registered in the United Kingdom, aiming to cultivate interdisciplinary research and integrated talents. We thank Kevin Liao for helping us improve the visual quality of this paper.

References

[1] M. Westerkamp and A. Küpper, "SmartSync: Cross-Blockchain Smart Contract Interaction and Synchronization," in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2022, pp. 1–9.

[2] P. Gaži, A. Kiayias, and D. Zindros, "Proof-of-stake sidechains," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 139–156.

[3] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, "Sok: Communication across distributed ledgers," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, N. Borisov and C. Diaz, Eds. Berlin, Heidelberg: Springer, 2021, p. 3–36.

[4] P. Wegner, "Interoperability," *ACM Comput. Surv.*, vol. 28, no. 1, p. 285–287, mar 1996. [Online]. Available: https://doi.org/10.1145/234313.234424

[5] D. Engel, M. Herlihy, and Y. Xue, "Failure is (literally) an Option: Atomic Commitment vs Optionality in Decentralized Finance," in *Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021, Virtual Event, November 17–20, 2021, Proceedings*. Berlin, Heidelberg: Springer-Verlag, Nov. 2021, pp. 66–77. [Online]. Available: https://doi.org/10.1007/978-3-030-91081-5_5

[6] V. Buterin, "Chain interoperability," *R3 research paper*, vol. 9, pp. 1–25, 2016.

[7] R. Belchior, L. Riley, T. Hardjono, A. Vasconcelos, and M. Correia, "Do You Need a Distributed Ledger Technology Interoperability Solution?" *Distributed Ledger Technologies: Research and Practice*, Sep. 2022, just Accepted. [Online]. Available: https://doi.org/10.1145/3564532

[8] R. Belchior, J. Süßenguth, Q. Feng, T. Hardjono, A. Vasconcelos, and M. Correia, "A brief history of blockchain interoperability," *Communications of the ACM*, Sep. 2024, accepted for publication.

[9] G. Wang, "Sok: Exploring blockchains interoperability," *Cryptology ePrint Archive*, 2021.

[10] G. Wang, Q. Wang, and S. Chen, "Exploring Blockchains Interoperability: A Systematic Survey," *ACM Computing Surveys*, p. 3582882, Feb. 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3582882

[11] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A Survey on Blockchain Interoperability: Past, Present, and Future Trends," *ACM Computing Surveys*, vol. 54, no. 8, pp. 168:1–168:41, Oct. 2021. [Online]. Available: https://doi.org/10.1145/3471140

[12] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, and W. Han, "An Overview on Cross-chain: Mechanism, Platforms, Challenges and Advances," *Computer Networks*, p. 109378, Sep. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128622004121

[13] L. Duan, Y. Sun, W. Ni, W. Ding, J. Liu, and W. Wang, "Attacks against cross-chain systems and defense approaches: A contemporary survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 10, no. 8, pp. 1643–1663, 2023.

[14] L. Li, J. Wu, and W. Cui, "A review of blockchain cross-chain technology," *IET Blockchain*, 2023.

[15] H. Mao, T. Nie, H. Sun, D. Shen, and G. Yu, "A Survey on Cross-Chain Technology: Challenges, Development, and Prospect," *IEEE Access*, vol. 11, pp. 45 527–45 546, 2023, conference Name: IEEE Access.

[16] G. Wang, Q. Wang, and S. Chen, "Exploring blockchains interoperability: A systematic survey," *ACM Computing Surveys*, p. 3582882, Feb 2023.

[17] T. Haugum, B. Hoff, M. Alsadi, and J. Li, "Security and Privacy Challenges in Blockchain Interoperability - A Multivocal Literature Review," in *Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022*, ser. EASE '22. New York, NY, USA: Association for Computing Machinery, Jun. 2022, pp. 347–356. [Online]. Available: https://doi.org/10.1145/3530019.3531345

[18] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to Scalability of Blockchain: A Survey," *IEEE Access*, vol. 8, pp. 16 440–16 455, 2020, conference Name: IEEE Access.

[19] R. Belchior, L. Riley, T. Hardjono, A. Vasconcelos, and M. Correia, "Do you need a distributed ledger technology interoperability solution?" *Distrib. Ledger Technol.*, vol. 2, no. 1, mar 2023. [Online]. Available: https://doi.org/10.1145/3564532

[20] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, Jan. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804518303485

[21] Y. Lan, J. Gao, Y. Li, K. Wang, Y. Zhu, and Z. Chen, "Trustcross: Enabling confidential interoperability across blockchains using trusted hardware," in *2021 4th International Conference on Blockchain Technology and Applications*. Xi'an China: ACM, Dec 2021, p. 17–23. [Online]. Available: https://dl.acm.org/doi/10.1145/3510487.3510491

[22] G. Almashaqbeh and R. Solomon, "Sok: Privacy-preserving computing in the blockchain era," in *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, Jun 2022, p. 124–139.

[23] "Top crypto bounty and ransom payments report," 2022. [Online]. Available: https://assets.ctfassets.net/t3wqy70tc3bv/6Tqb2wlVnwdGYeVZX4WDmU/6b0c222b4f680ac80ea801e032894eac/Immunefi_Crypto_Bug_Bounty_and_Ransom_Payments_Report.pdf

[24] "Largest defi exploits." [Online]. Available: https://www.theblock.co/data/decentralized-finance/exploits/largest-defi-exploits

[25] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "Sok: Decentralized finance (defi) attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 2444–2461.

[26] "Rekt - leaderboard." [Online]. Available: https://www.rekt.news/

[27] "Rekt - multichain - rekt 2." [Online]. Available: https://rekt.news/multichain-rekt2/

[28] C. Team, "Multichain exploit: Possible hack or rug pull," Jul 2023. [Online]. Available: https://www.chainalysis.com/blog/multichain-exploit-july-2023/

[29] A. [@Allbridge_io], "We are investigating the current situation with the bnb chain pools. the bridge has been temporarily shut down during the investigation. we apologize for the inconvenience." Apr 2023. [Online]. Available: https://twitter.com/Allbridge_io/status/1642341041410908164

[30] S. Reynolds, "Mixin network losses nearly $200m in hack," Sep. 2023. [Online]. Available: https://www.coindesk.com/tech/2023/09/25/mixin-network-losses-nearly-200m-in-hack/

[31] "The chainalysis 2023 crypto crime report," Feb. 2023.

[32] "L2beat – the state of the layer two ecosystem." [Online]. Available: https://l2beat.com/bridges/summary

[33] J. Su, J. Liu, Y. Nan, and Y. Li, "Security Evaluation of Smart Contracts based on Code and Transaction - A Survey," in *2022 International Conference on Service Science (ICSS)*, May 2022, pp. 41–48.

[34] "Interoperability modes | weaver." [Online]. Available: https://hyperledger-labs.github.io/weaver-dlt-interoperability/docs/external/interoperability-modes/

[35] V. Ramakrishna, "Secure asset transfer protocol (satp) future extensions: Asset and process state queries," IETF 117: Secure Asset Transfer Working Group, Jul. 2023. [Online]. Available: https://datatracker.ietf.org/meeting/117/materials/slides-117-satp-sharing-of-asset-state-and-process-snapshot-views-01

[36] E. Abebe, D. Behl, C. Govindarajan, Y. Hu, D. Karunamoorthy, P. Novotny, V. Pandit, V. Ramakrishna, and C. Vecchiola, "Enabling enterprise blockchain interoperability with trusted data transfer (industry track)," in *Proceedings of the 20th International Middleware Conference Industrial Track*. Davis CA USA: ACM, Dec 2019, p. 29–35. [Online]. Available: https://dl.acm.org/doi/10.1145/3366626.3368129

[37] G. Wang, Q. Wang, and S. Chen, "Exploring blockchains interoperability: A systematic survey," *ACM Computing Surveys*, 2023.

[38] P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte, "ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains," in *2020 IEEE International Conference on Blockchain (Blockchain)*, Nov. 2020, pp. 204–213.

[39] O. Ciobotaru, F. Shirazi, A. Stewart, and S. Vasilyev, "Accountable light client systems for pos blockchains," Cryptology ePrint Archive, Paper 2022/1205, 2022, https://eprint.iacr.org/2022/1205. [Online]. Available: https://eprint.iacr.org/2022/1205

[40] R. Belchior, D. Dimov, Z. Karadjov, J. Pfannschmidt, A. Vasconcelos, and M. Correia, "Harmonia: Securing cross-chain applications using zero-knowledge proofs," 2024.

[41] T. Xie, J. Zhang, Z. Cheng, F. Zhang, Y. Zhang, Y. Jia, D. Boneh, and D. Song, "zkBridge: Trustless Cross-chain Bridges Made Practical," Oct. 2022, arXiv:2210.00264 [cs]. [Online]. Available: http://arxiv.org/abs/2210.00264

[42] M. Westerkamp and J. Eberhardt, "zkRelay: Facilitating Sidechains using zkSNARK-based Chain-Relays," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Sep. 2020, pp. 378–386.

[43] R. Belchior, L. Torres, J. Pfannschmid, A. Vasconcelos, and M. Correia, "Can we share the same perspective? blockchain interoperability with views," Oct. 2022. [Online]. Available: http://dx.doi.org/10.36227/techrxiv.20025857.v3

[44] M. Hargreaves, T. Hardjono, and R. Belchior, "Secure asset transfer protocol (satp)," Jul 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-satp-core

[45] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais, and W. Knottenbelt, "XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets," in *2019 IEEE Symposium on Security and Privacy (SP)*, May 2019, pp. 193–210, iSSN: 2375-1207.

[46] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE Access*, vol. 7, pp. 28 712–28 725, 2019.

[47] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2020.

[48] E. Abebe, P. Robinson, A. Chand, M. Murdock, and D. Hyland-Wood, "Crosschain Risk Framework." [Online]. Available: https://crosschainriskframework.github.io/

[49] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Jan. 2004, conference Name: IEEE Transactions on Dependable and Secure Computing.

[50] E. J. Scheid, T. Hegnauer, B. Rodrigues, and B. Stiller, "Bifröst: a modular blockchain interoperability api," in *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, Oct 2019, p. 332–339.

[51] S. Ghaemi, S. Rouhani, R. Belchior, R. S. Cruz, H. Khazaei, and P. Musilek, "A pub-sub architecture to promote blockchain interoperability," 2021.

[52] Y. Tao, B. Li, and B. Li, "On atomicity and confidentiality across blockchains under failures," *IEEE Transactions on Knowledge and Data Engineering*, p. 1–14, 2023.

[53] L. Vishwakarma, A. Kumar, and D. Das, "Crossledger: A pioneer cross-chain asset transfer protocol," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*, May 2023, p. 568–578.

[54] Y. Zhang, S. Hu, Q. Wang, B. Qin, Q. Wu, and W. Shi, "PXCrypto: A Regulated Privacy-Preserving Cross-Chain Transaction Scheme," in *Algorithms and Architectures for Parallel Processing*, ser. Lecture Notes in Computer Science, W. Meng, R. Lu, G. Min, and J. Vaidya, Eds. Cham: Springer Nature Switzerland, 2023, pp. 170–191.

[55] R. Belchior, A. Vasconcelos, M. Correia, and T. Hardjono, "Hermes: Fault-tolerant middleware for blockchain interoperability," *Future Generation Computer Systems*, vol. 129, pp. 236–251, Apr. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X21004337

[56] D. Patel, H. Anand, and S. Chakraborty, "CrossTrustchain: Cross-Chain Interoperability using Multivariate Trust Models," in *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, Jan. 2023, pp. 129–134, iSSN: 2155-2509.

[57] S. Zhang, T. Xie, K. Gai, and L. Xu, "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)*, Jun. 2022, pp. 86–92, iSSN: 2693-8928.

[58] O. Shlomovits and O. Leiba, "JugglingSwap: Scriptless Atomic Cross-Chain Swaps," Jul. 2020, arXiv:2007.14423 [cs]. [Online]. Available: http://arxiv.org/abs/2007.14423

[59] B. Dai, S. Jiang, M. Zhu, M. Lu, D. Li, and C. Li, "Research and implementation of cross-chain transaction model based on improved hash-locking," in *Blockchain and Trustworthy Systems*, ser. Communications in Computer and Information Science, Z. Zheng, H.-N. Dai, X. Fu, and B. Chen, Eds. Singapore: Springer, 2020, p. 218–230.

[60] M. Li, J. Weng, Y. Li, Y. Wu, J. Weng, D. Li, G. Xu, and R. Deng, "IvyCross: A Privacy-Preserving and Concurrency Control Framework for Blockchain Interoperability," 2021, report Number: 1244. [Online]. Available: https://eprint.iacr.org/2021/1244

[61] G. Wang and M. Nixon, "InterTrust: Towards an Efficient Blockchain Interoperability Architecture with Trusted Services," in *2021 IEEE International Conference on Blockchain (Blockchain)*, Dec. 2021, pp. 150–159.

[62] I. Bentov, Y. Ji, F. Zhang, L. Breidenbach, P. Daian, and A. Juels, "Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, Nov. 2019, pp. 1521–1538. [Online]. Available: https://doi.org/10.1145/3319535.3363221

[63] V. Zakhary, D. Agrawal, and A. El Abbadi, "Atomic commitment across blockchains," *Proceedings of the VLDB Endowment*, vol. 13, no. 9, p. 1319–1331, May 2020.

[64] Y. Li, J. Weng, M. Li, W. Wu, J. Weng, J.-N. Liu, and S. Hu, "ZeroCross: A sidechain-based privacy-preserving Cross-chain solution for Monero," *Journal of Parallel and Distributed Computing*, vol. 169, pp. 301–316, Nov. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0743731522001733

[65] M. D. Montiel, R. Guerraoui, and P.-L. Roman, "SurferMonkey: A Decentralized Anonymous Blockchain Intercommunication System via Zero Knowledge Proofs," Oct. 2022, arXiv:2210.13242 [cs]. [Online]. Available: http://arxiv.org/abs/2210.13242

[66] W. Liu, Z. Wan, J. Shao, and Y. Yu, "HyperMaze: Towards Privacy-Preserving and Scalable Permissioned Blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 360–376, Jan. 2023, conference Name: IEEE Transactions on Dependable and Secure Computing.

[67] X. Pang, N. Kong, and Z. Chen, "AbitBridge: A cross-chain protocol based on main-sub-chain architecture," in *2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE)*, Sep. 2022, pp. 99–104, iSSN: 2770-663X.

[68] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, and Y.-C. Hu, "HyperService: Interoperability and Programmability Across Heterogeneous Blockchains," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. London United Kingdom: ACM, Nov. 2019, pp. 549–566. [Online]. Available: https://dl.acm.org/doi/10.1145/3319535.3355503

[69] B. C. Ghosh, T. Bhartia, S. K. Addya, and S. Chakraborty, "Leveraging Public-Private Blockchain Interoperability for Closed Consortium Interfacing," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*, May 2021, pp. 1–10, iSSN: 2641-9874.

[70] Y. Sun, L. Yi, L. Duan, and W. Wang, "A Decentralized Cross-Chain Service Protocol based on Notary Schemes and Hash-Locking," in *2022 IEEE International Conference on Services Computing (SCC)*, Jul. 2022, pp. 152–157, iSSN: 2474-2473.

[71] M. Sober, G. Scaffino, C. Spanring, and S. Schulte, "A Voting-Based Blockchain Interoperability Oracle," Nov. 2021, arXiv:2111.10091 [cs]. [Online]. Available: http://arxiv.org/abs/2111.10091

[72] H. Tian, K. Xue, X. Luo, S. Li, J. Xu, J. Liu, J. Zhao, and D. S. L. Wei, "Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3928–3941, 2021, conference Name: IEEE Transactions on Information Forensics and Security.

[73] Y. Yang, F. Bai, Z. Yu, T. Shen, Y. Liu, and B. Gong, "An Anonymous and Supervisory Cross-Chain Privacy Protection Protocol for Zero-Trust IoT Application," *ACM Transactions on Sensor Networks*, p. 3583073, Mar. 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3583073

[74] Z. Yin, B. Zhang, J. Xu, K. Lu, and K. Ren, "Bool Network: An Open, Distributed, Secure Cross-Chain Notary Platform," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3465–3478, 2022, conference Name: IEEE Transactions on Information Forensics and Security.

[75] F. Barbàra and C. Schifanella, "BxTB: cross-chain exchanges of bitcoins for all Bitcoin wrapped tokens," in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, Sep. 2022, pp. 143–150.

[76] M. Westerkamp and M. Diez, "Verilay: A Verifiable Proof of Stake Chain Relay," in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, May 2022, pp. 1–9, arXiv:2201.08697 [cs]. [Online]. Available: http://arxiv.org/abs/2201.08697

[77] A. Sanchez, A. Stewart, and F. Shirazi, "Bridging Sapling: Private Cross-Chain Transfers," in *2022 IEEE Crosschain Workshop (ICBC-CROSS)*, May 2022, pp. 1–9.

[78] D. Stone, "Trustless, privacy-preserving blockchain bridges," Feb. 2021, arXiv:2102.04660 [cs]. [Online]. Available: http://arxiv.org/abs/2102.04660

[79] A. Li, G. D'Angelo, J. Tang, F. Fang, and B. Gong, "An auditable confidentiality protocol for blockchain transactions," Cryptology ePrint Archive, Paper 2022/1672, 2022. [Online]. Available: https://eprint.iacr.org/2022/1672

[80] Y. Xue and M. Herlihy, "Hedging Against Sore Loser Attacks in Cross-Chain Transactions," in *Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing*, ser. PODC'21. New York, NY, USA: Association for Computing Machinery, Jul. 2021, pp. 155–164. [Online]. Available: https://doi.org/10.1145/3465084.3467904

[81] X. Zhang, J. Chen, Y. Zhou, and S. Jiang, "Privacy-Preserving Cross-Chain Payment Scheme for Blockchain-Enabled Energy Trading," in *2021 IEEE/CIC International Conference on Communications in China (ICCC)*, Jul. 2021, pp. 109–114, iSSN: 2377-8644.

[82] D. Ding, B. Long, F. Zhuo, Z. Li, H. Zhang, C. Tian, and Y. Sun, "Lilac: Parallelizing Atomic Cross-Chain Swaps," in *2022 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2022, pp. 1–8, iSSN: 2642-7389.

[83] T. Bugnet and A. Zamyatin, "XCC: Theft-Resilient and Collateral-Optimized Cryptocurrency-Backed Assets," 2022, report Number: 113. [Online]. Available: https://eprint.iacr.org/2022/113

[84] I. Tsabary, M. Yechieli, A. Manuskin, and I. Eyal, "MAD-HTLC: Because HTLC is Crazy-Cheap to Attack," in *2021 IEEE Symposium on Security and Privacy (SP)*, May 2021, pp. 1230–1248, iSSN: 2375-1207.

[85] M. Herlihy, "Atomic Cross-Chain Swaps," in *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*. Egham United Kingdom: ACM, Jul. 2018, pp. 245–254. [Online]. Available: https://dl.acm.org/doi/10.1145/3212734.3212736

[86] S. Mazumdar, "Towards faster settlement in htlc-based cross-chain atomic swaps," in *2022 IEEE 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. Los Alamitos, CA, USA: IEEE Computer Society, dec 2022, pp. 295–304. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/TPS-ISA56441.2022.00043

[87] A. Deshpande and M. Herlihy, "Privacy-Preserving Cross-Chain Atomic Swaps," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, M. Bernhard, A. Bracciali, L. J. Camp, S. Matsuo, A. Maurushat, P. B. Rønne, and M. Sala, Eds. Cham: Springer International Publishing, 2020, pp. 540–549.

[88] J. Cai, Y. Zhou, T. Hu, and B. Li, "PTLC: Protect the Identity Privacy during Cross-Chain Asset Transaction More Effectively," in *2022 IEEE 22nd International Conference on Software Quality, Reliability, and Security Companion (QRS-C)*, Dec. 2022, pp. 70–78, iSSN: 2693-9371.

[89] J. Kirsten and H. Davarpanah, "Anonymous Atomic Swaps Using Homomorphic Hashing," Rochester, NY, Aug. 2018. [Online]. Available: https://papers.ssrn.com/abstract=3235955

[90] K. Narayanam, V. Ramakrishna, D. Vinayagamurthy, and S. Nishad, "Atomic cross-chain exchanges of shared assets," in *Proceedings of the 4th ACM Conference on Advances in Financial Technologies*, ser. AFT '22. New York, NY, USA: Association for Computing Machinery, 2023, p. 148–160. [Online]. Available: https://doi.org/10.1145/3558535.3559786

[91] S. A. Thyagarajan, G. Malavolta, and P. Moreno-Sánchez, "Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains," 2021, report Number: 1612. [Online]. Available: https://eprint.iacr.org/2021/1612

[92] R. Li, Y. Xie, Z. Ning, C. Zhang, and L. Wei, "Privacy-Preserving Decentralized Cryptocurrency Exchange without Price Manipulation," in *2022 IEEE/CIC International Conference on Communications in China (ICCC)*, Aug. 2022, pp. 274–279, iSSN: 2377-8644.

[93] L. Hanzlik, J. Loss, S. A. Thyagarajan, and B. Wagner, "Sweep-uc: Swapping coins privately," Cryptology ePrint Archive, Paper 2022/1605, 2022. [Online]. Available: https://eprint.iacr.org/2022/1605

[94] Y. Manevich and A. Akavia, "Cross Chain Atomic Swaps in the Absence of Time via Attribute Verifiable Timed Commitments," in *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, Jun. 2022, pp. 606–625.

[95] A. Augusto, R. Belchior, I. Kocsis, L. Gönczy, A. Vasconcelos, and M. Correia, "Cbdc bridging between hyperledger fabric and permissioned evm-based blockchains," in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1–9.

[96] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 57–64.

[97] A. Labs, "Avalanche bridge." [Online]. Available: https://core.app/bridge/

[98] "Why trusted execution environments will be integral to proof-of-stake blockchains," Jun 2022. [Online]. Available: https://venturebeat.com/datadecisionmakers/why-trusted-execution-environments-will-be-integral-to-proof-of-stake-blockchains/

[99] "What is the role of the avalanche bridge nodes?" [Online]. Available: https://support.avax.network/en/articles/5462271-what-is-the-role-of-the-avalanche-bridge-nodes

[100] P. Jauernig, A.-R. Sadeghi, and E. Stapf, "Trusted execution environments: Properties, applications, and challenges," *IEEE Security & Privacy*, vol. 18, no. 2, pp. 56–60, 2020.

[101] E. Helmore, "Crypto giant binance admits to money laundering and agrees to pay $4.3bn," *The Guardian*, Nov. 2023. [Online]. Available: https://www.theguardian.com/business/2023/nov/21/binance-settlement-crypto-exchange

[102] "Coinex faces a major security breach with $27 million estimated loss – cryptopolitan." [Online]. Available: https://www.cryptopolitan.com/coinex-faces-a-major-security-breach/

[103] "Announcement | Binance Security Breach Update." [Online]. Available: https://www.binance.com/en/support/announcement/binance-security-breach-update-360028031711

[104] "Axelar Network: Connecting Applications with Blockchain Ecosystems," 2021. [Online]. Available: https://axelar.network/axelar_whitepaper.pdf

[105] "The value layer of the internet." [Online]. Available: https://polygon.technology/

[106] M. Herlihy, B. Liskov, and L. Shrira, "Cross-chain deals and adversarial commerce," *The VLDB Journal*, vol. 31, no. 6, pp. 1291–1309, Nov. 2022. [Online]. Available: https://doi.org/10.1007/s00778-021-00686-1

[107] "Bridge assesment report – uniswap foundation." [Online]. Available: https://uniswap.notion.site/Bridge-Assessment-Report-0c8477afadce425abac9c0bd175ca382

[108] "Portal token bridge." [Online]. Available: https://portalbridge.com

[109] "Wanchain – we are all connected." [Online]. Available: https://docs.wanchain.org/get-started/introduction

[110] "Btc relay." [Online]. Available: http://btcrelay.org/

[111] "Minimal light client." [Online]. Available: https://github.com/ethereum/annotated-spec/blob/master/altair/sync-protocol.md

[112] J. Groth, "On the size of pairing-based non-interactive arguments," in *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II 35*. Springer, 2016, pp. 305–326.

[113] "zksync — accelerating the mass adoption of crypto for personal sovereignty." [Online]. Available: https://zksync.io/

[114] "Scroll - native zkevm layer 2 for ethereum." [Online]. Available: https://scroll.io/

[115] "Taiko." [Online]. Available: https://taiko.xyz/

[116] Bhuptani, Arjun, "Optimistic Bridges: A New Paradigm for Crosschain Communication," 2022. [Online]. Available: https://blog.connext.network/optimistic-bridges-fb800dc7b0e0

[117] "Optimism." [Online]. Available: https://www.optimism.io/

[118] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain Scaling Using Rollups: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 93 039–93 054, 2022, conference Name: IEEE Access.

[119] D. Boneh and M. Naor, "Timed commitments," in *Advances in Cryptology — CRYPTO 2000*, ser. Lecture Notes in Computer Science, M. Bellare, Ed. Berlin, Heidelberg: Springer, 2000, p. 236–254.

[120] S. A. K. Thyagarajan, A. Bhat, G. Malavolta, N. Döttling, A. Kate, and D. Schröder, "Verifiable timed signatures made practical," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1733–1750. [Online]. Available: https://doi.org/10.1145/3372297.3417263

[121] R. Han, H. Lin, and J. Yu, "On the optionality and fairness of atomic swaps," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, ser. AFT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 62–75. [Online]. Available: https://doi.org/10.1145/3318041.3355460

[122] J. Xu, D. Ackerer, and A. Dubovitskaya, "A Game-Theoretic Analysis of Cross-Chain Atomic Swaps with HTLCs," in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*, Jul. 2021, pp. 584–594, iSSN: 2575-8411.

[123] Y. Xue, D. Jin, and M. Herlihy, "Invited Paper: Fault-tolerant and Expressive Cross-Chain Swaps," Nov. 2022, arXiv:2211.00208 [cs]. [Online]. Available: http://arxiv.org/abs/2211.00208

[124] E. Chan, M. Chrobak, and M. Lesani, "Cross-chain Swaps with Preferences," Oct. 2022, arXiv:2210.11791 [cs]. [Online]. Available: http://arxiv.org/abs/2210.11791

[125] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[126] Z. Wang, S. Chaliasos, K. Qin, L. Zhou, L. Gao, P. Berrang, B. Livshits, and A. Gervais, "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy," in *Proceedings of the ACM Web Conference 2023*, 2023, pp. 2022–2032.

[127] F. Victor and A. M. Weintraud, "Detecting and quantifying wash trading on decentralized cryptocurrency exchanges," in *Proceedings of the Web Conference 2021*, ser. WWW '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 23–32. [Online]. Available: https://doi.org/10.1145/3442381.3449824

[128] D. Chaum, "Blind signature system," in *Advances in Cryptology: Proceedings of Crypto 83*. Springer, 1983, pp. 153–153.

[129] N. Alsalami and B. Zhang, "SoK: A Systematic Study of Anonymity in Cryptocurrencies," in *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, Nov. 2019, pp. 1–9.

[130] L. Wang, G. Zhang, and C. Ma, "A survey of ring signature," *Frontiers of Electrical and Electronic Engineering in China*, vol. 3, no. 1, p. 10–19, Jan. 2008.

[131] J. Lv and X. Wang, "Verifiable ring signature," in *Proc. of DMS 2003-The 9th International Conference on Distribted Multimedia Systems*, 2003, pp. 663–667.

[132] "Polygon." [Online]. Available: https://wiki.polygon.technology/

[133] "Optmism." [Online]. Available: https://community.optimism.io/docs/developers/bridge/basics.html

[134] "Arbitrum." [Online]. Available: https://docs.arbitrum.io/devs-how-tos/bridge-tokens/how-to-bridge-tokens-overview

[135] "Ronin." [Online]. Available: https://docs.roninchain.com/docs/basics/dapps/ronin-bridge

[136] "zksync - bridging." [Online]. Available: https://era.zksync.io/docs/reference/concepts/bridging-asset.html

[137] "Connext." [Online]. Available: https://docs.connext.network/concepts/readme

[138] L. Zhang, X. Ma, and Y. Liu, "Sok: Blockchain decentralization," *arXiv preprint arXiv:2205.04256*, 2022.

[139] R. Belchior, S. Scuri, I. Mihaiu, N. Nunes, and T. Hardjono, "Towards a common standard framework for blockchain interoperability - a position paper," Oct. 2023. [Online]. Available: http://dx.doi.org/10.36227/techrxiv.17093039.v4

[140] R. Zarick, B. Pellegrino, and C. Banister, "Layerzero: Trustless omnichain interoperability protocol," 2021.

[141] W. Foundation, "wormhole/SECURITY.md at main · wormhole-foundation/wormhole — github.com," https://github.com/wormhole-foundation/wormhole/blob/main/SECURITY.md, [Accessed 07-Jul-2023].

[142] J. Swihart, B. Winston, and S. Bowe, "Zcash counterfeiting vulnerability successfully remediated," *Retrieved November*, vol. 20, p. 2019, 2019.

[143] M. Wu, W. McTighe, K. Wang, I. A. Seres, N. Bax, M. Puebla, M. Mendez, F. Carrone, T. D. Mattey, H. O. Demaestri, M. Nicolini, and P. Fontana, "Tutela: An open-source tool for assessing user-privacy on ethereum and tornado cash," 2022.

[144] "The Monero project." [Online]. Available: https://www.getmonero.org/index.html

[145] "Tornado cash." [Online]. Available: https://github.com/tornadocash

[146] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in *Proceedings of the 28th USENIX Conference on Security Symposium*, ser. SEC'19. USA: USENIX Association, Aug. 2019, pp. 837–850.

[147] Q. Wang, B. Qin, J. Hu, and F. Xiao, "Preserving transaction privacy in bitcoin," *Future Generation Computer Systems*, vol. 107, pp. 793–804, Jun. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17318393

[148] H. Xie, S. Fei, Z. Yan, and Y. Xiao, "SofitMix: A Secure Offchain-Supported Bitcoin-Compatible Mixing Protocol," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–15, 2022, conference Name: IEEE Transactions on Dependable and Secure Computing.

[149] F. A. Hayek, M. Koscina, P. Lafourcade, and C. Olivier-Anclin, "Generic Privacy Preserving Private Permissioned Blockchains," in *The 38th ACM/SIGAPP Symposium On Applied Computing*, Tallinn, Estonia, Mar. 2023. [Online]. Available: https://hal.uca.fr/hal-03906880

[150] "Celestia." [Online]. Available: https://celestia.org/

[151] "Arbitrum audit." [Online]. Available: https://github.com/ArbitrumFoundation/governance/blob/main/audits/trail_of_bits_governance_report_1_6_2023.pdf

[152] S.-S. Lee, A. Murashkin, M. Derka, and J. Gorzny, "SoK: Not Quite Water Under the Bridge: Review of Cross-Chain Bridge Hacks," Oct. 2022, arXiv:2210.16209 [cs]. [Online]. Available: http://arxiv.org/abs/2210.16209

[153] R. Belchior, P. Somogyvari, J. Pfannschmid, A. Vasconcelos, and M. Correia, "Hephaestus: Modelling, analysis, and performance evaluation of cross-chain transactions," Nov. 2023. [Online]. Available: http://dx.doi.org/10.36227/techrxiv.20718058.v3

[154] J. Zhang, J. Gao, Y. Li, Z. Chen, Z. Guan, and Z. Chen, "Xscope: Hunting for cross-chain bridge attacks," in *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, ser. ASE '22. New York, NY, USA: Association for Computing Machinery, 2023. [Online]. Available: https://doi.org/10.1145/3551349.3559520

[155] "zkrouter," Nov. 2022. [Online]. Available: https://drive.google.com/file/d/1ibuHChcYcYCN6JelRAQPnM4rkaB9EgAM

[156] "Axie infinity bridge audit." [Online]. Available: https://docs.roninchain.com/assets/files/CertiK-Audit-for-Axie-Infinity---Audit-v8-1bfcb82b195442bf34a28ed2fdbde6c5.pdf

[157] Z. Lv, D. Wu, W. Yang, and L. Duan, "Attack and protection schemes on fabric isomorphic crosschain systems," *International Journal of Distributed Sensor Networks*, vol. 18, no. 1, p. 15501477211059945, Jan. 2022, publisher: SAGE Publications. [Online]. Available: https://doi.org/10.1177/15501477211059945

[158] Jun 2022. [Online]. Available: https://aurora.dev/blog/aurora-mitigates-its-inflation-vulnerability

[159] "Starknet dai bridge audit." [Online]. Available: https://chainsecurity.com/wp-content/uploads/2021/12/ChainSecurity_MakerDAO_StarkNet-DAI-Bridge_audit.pdf

[160] T. Eizinger, P. Hoenisch, and L. S. del Pino, "Open problems in cross-chain protocols," Jan. 2021, arXiv:2101.12412 [cs]. [Online]. Available: http://arxiv.org/abs/2101.12412

[161] "Message traps in the arbitrum bridge," 2022. [Online]. Available: https://www.notonlyowner.com/research/message-traps-in-the-arbitrum-bridge

[162] "Circle audit." [Online]. Available: https://chainsecurity.com/wp-content/uploads/2023/04/Circle-Smart-Contract-Audit-_-Cross-Chain-Transfer-Protocol-CCTP-_-EVM-Bridge-_-ChainSecurity.pdf

[163] P. McCorry, C. Buckland, B. Yee, and D. Song, "Sok: Validating bridges as a scaling solution for blockchains," Cryptology ePrint Archive, Paper 2021/1589, 2021. [Online]. Available: https://eprint.iacr.org/2021/1589

[164] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "Sok: Decentralized finance (defi)," *arXiv preprint arXiv:2101.08778*, 2021.

[165] T. Mackinga, T. Nadahalli, and R. Wattenhofer, "Twap oracle attacks: Easier done than said?" in *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2022, pp. 1–8.

[166] K. Tjiam, R. Wang, H. Chen, and K. Liang, "Your smart contracts are not secure: investigating arbitrageurs and oracle manipulators in ethereum," in *Proceedings of the 3rd Workshop on Cyber-Security Arms Race*, 2021, pp. 25–35.

[167] S. Eskandari, M. Salehi, W. C. Gu, and J. Clark, "Sok: Oracles from the ground truth to market manipulation," in *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies*, 2021, pp. 127–141.

[168] Q. Finance, "Protocol exploit report," Jan 2022. [Online]. Available: https://medium.com/@QubitFin/protocol-exploit-report-305c34540fa3

[169] "Rekt - meter." [Online]. Available: https://rekt.news/meter-rekt/

[170] "Rekt - nomad bridge." [Online]. Available: https://rekt.news/nomad-rekt/

[171] THORChain, "Eth parsing error and exploit," Jun 2021. [Online]. Available: https://medium.com/thorchain/eth-parsing-error-and-exploit-3b343aa6466f

[172] M. Gupta, "Poly network hack analysis - largest crypto hack," Aug 2021. [Online]. Available: https://mudit.blog/poly-network-largest-crypto-hack/

[173] "Rekt - bnb bridge." [Online]. Available: https://www.rekt.news/bnb-bridge-rekt/

[174] C. [@CelerNetwork], "(1/n)a DNS cache poisoning attack on cbridge's frontend ui approx..." Aug 2022. [Online]. Available: https://twitter.com/CelerNetwork/status/1560123830844411904

[175] "Multichain contract vulnerability post mortem | by multichain (previously anyswap) | medium." [Online]. Available: https://medium.com/multichainorg/multichain-contract-vulnerability-post-mortem-d37bfab237c8

[176] "Wormhole audit." [Online]. Available: https://github.com/wormhole-foundation/wormhole-audits/blob/main/Wormhole_Audit_Report_TrailOfBits_2022-09.pdf

[177] "Wormhole audit." [Online]. Available: https://github.com/trailofbits/publications/blob/master/reviews/2023-03-wormhole-securityreview.pdf

[178] "Polygon pos audit." [Online]. Available: https://chainsecurity.com/wp-content/uploads/2023/04/Polygon_PoS_Portal_-Smart-Contract-Audit_ChainSecurity.pdf

[179] "Wormhole audit." [Online]. Available: https://github.com/wormhole-foundation/wormhole-audits/blob/main/2023-03-08_CertiK_Wormhole_EVM.pdf

[180] "zksync dai bridge audit." [Online]. Available: https://chainsecurity.com/wp-content/uploads/2023/08/ChainSecurity_MakerDAO_zkSync_DAI_Bridge_audit.pdf

[181] "Using with upgrades - openzeppelin docs." [Online]. Available: https://docs.openzeppelin.com/contracts/3.x/upgradeable

[182] 0xriptide, "Hackers in arbitrum's inbox," Sep 2022. [Online]. Available: https://medium.com/@0xriptide/hackers-in-arbitrums-inbox-ca23272641a2

[183] "Report on Crypto Exchange Hacks." [Online]. Available: https://cointelegraph.com/magazine/crypto-exchange-hacks/

[184] Mar 2023. [Online]. Available: https://cointelegraph.com/news/arbitrum-discord-hacker-shares-phishing-announcement-amid-airdrop-hype

[185] S. Singh Sidhu, M. N. H. Nguyen, C. Ngene, and S. Rouhani, "Trust development for blockchain interoperability using self-sovereign identity integration," in *2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct 2022, p. 0033–0040.

[186] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten, "Arbitrum: scalable, private smart contracts," in *Proceedings of the 27th USENIX Conference on Security Symposium*, ser. SEC'18. USA: USENIX Association, Aug 2018, p. 1353–1370.

[187] A. Pupyshev, D. Gubanov, E. Dzhafarov, I. Sapranidi, I. Kardanov, V. Zhuravlev, S. Khalilov, M. Jansen, S. Laureyssens, I. Pavlov, and S. Ivanov, "Gravity: a blockchain-agnostic cross-chain communication and data oracles protocol," Aug. 2020, arXiv:2007.00966 [cs]. [Online]. Available: http://arxiv.org/abs/2007.00966

[188] A. Rondelet and Q. Kilbourn, "Threshold encrypted mempools: Limitations and considerations," 2023.

[189] K. Qin, L. Zhou, and A. Gervais, "Quantifying Blockchain Extractable Value: How dark is the forest?" Dec. 2021, arXiv:2101.05511 [cs]. [Online]. Available: http://arxiv.org/abs/2101.05511

[190] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses," *ACM Computing Surveys*, vol. 53, no. 3, pp. 67:1–67:43, Jun. 2020. [Online]. Available: https://doi.org/10.1145/3391195

[191] F. Barbàra and C. Schifanella, "Mp-htlc: Enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 9, p. e7656, 2023.

[192] "Slither: the Solidity source analyzer," May 2023. [Online]. Available: https://github.com/crytic/slither

[193] "Ronin bridge." [Online]. Available: https://bridge.roninchain.com/

[194] "Polybridge." [Online]. Available: https://bridge.poly.network/

[195] "Binance." [Online]. Available: https://www.binance.org/

[196] "Nomad | bridge." [Online]. Available: https://app.nomad.xyz/

[197] "Bxh." [Online]. Available: https://app.bxh.com/#/

[198] "Multichain - cross chain router protocol." [Online]. Available: https://app.multichain.org/#/router

[199] "Harmony one-eth bridge." [Online]. Available: https://bridge.harmony.one/one

[200] "Qubit." [Online]. Available: https://xbridge.qbt.fi

[201] "ptokens dapp." [Online]. Available: https://dapp.ptokens.io/#/swap?asset=btc&from=btc&to=eth

[202] "Thorchain." [Online]. Available: https://thorchain.org/

[203] "Meter passport." [Online]. Available: https://passport.meter.io/#/

[204] "Chainswap." [Online]. Available: https://exchange.chainswap.com/#/dashboard

[205] [Online]. Available: https://immunefi.com/explore/?filter=productType%3DCrosschain%2BLiquidity

[206] "List of btc addresses controlled by the pnetwork attacker." [Online]. Available: https://pastebin.com/raw/bAquZVws

[207] "Polynetwork and hacker communicate." [Online]. Available: https://docs.google.com/spreadsheets/u/1/d/11LUJwLoHX8ZCyfjhg5YZ0V99iU6PafMNL_NET45FSVc

[208] C. Team, "Poly network attacker returning funds after pulling off biggest defi theft ever," Aug 2021. [Online]. Available: https://blog.chainalysis.com/reports/poly-network-hack-august-2021/

[209] "Circle rolls out native usdc tokens on polygon," Oct. 2023. [Online]. Available: https://cointelegraph.com/news/circle-launches-usdc-tokens-on-polygon

[210] B. Putz, F. Böhm, and G. Pernul, *HyperSec: Visual Analytics for Blockchain Security Monitoring*, ser. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2021, vol. 625, p. 165–180. [Online]. Available: https://link.springer.com/10.1007/978-3-030-78120-0_11

[211] "Openzeppelin/openzeppelin-contracts," May 2023. [Online]. Available: https://github.com/OpenZeppelin/openzeppelin-contracts

[212] P. M. Caversaccio, "A historical collection of reentrancy attacks," May 2023, accessed on 12.09.2023. [Online]. Available: https://github.com/pcaversaccio/reentrancy-attacks

[213] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," Sep. 2022, arXiv:2101.08778 [cs, econ, q-fin]. [Online]. Available: http://arxiv.org/abs/2101.08778

[214] T. Krupa, M. Ries, I. Kotuliak, K. Košťál, and R. Bencel, "Security Issues of Smart Contracts in Ethereum Platforms," in *2021 28th Conference of Open Innovations Association (FRUCT)*, Jan. 2021, pp. 208–214, iSSN: 2305-7254.

[215] M. Fowler and M. Foemmel, "Continuous integration," 2006.

[216] "Mythril: Security analysis tool for EVM bytecode." [Online]. Available: https://github.com/ConsenSys/mythril

[217] "Mythx: Smart contract security service for ethereum." [Online]. Available: https://mythx.io/

[218] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, "A survey of smart contract formal specification and verification," *ACM Comput. Surv.*, vol. 54, no. 7, jul 2021. [Online]. Available: https://doi.org/10.1145/3464421

[219] "Echidna: A fast smart contract fuzzer," May 2023. [Online]. Available: https://github.com/crytic/echidna

[220] V. Wüstholz and M. Christakis, "Harvey: a greybox fuzzer for smart contracts," in *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. Virtual Event USA: ACM, Nov 2020, p. 1398–1409. [Online]. Available: https://dl.acm.org/doi/10.1145/3368089.3417064

[221] "Scribble," May 2023. [Online]. Available: https://github.com/ConsenSys/scribble

[222] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. Los Alamitos, CA, USA: IEEE Computer Society, oct 2001, p. 136. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SFCS.2001.959888

[223] L. Lamport, "Specifying systems: the tla+ language and tools for hardware and software engineers," 2002.

[224] G. Verdian, P. Tasca, C. Paterson, and G. Mondelli, "Quant overledger whitepaper," *Release V0*, vol. 1, p. 31, 2018.

[225] J. Kwon and E. Buchman, "Cosmos whitepaper," *A Netw. Distrib. Ledgers*, vol. 27, 2019.

[226] C. McMenamin, "Sok: Cross-domain mev," 2023.

[227] E. C. Bank. (2023) Eurosystem proceeds to next phase of digital euro project. Accessed on 16 October 2023. [Online]. Available: https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html

[228] B. Pillai, K. Biswas, Z. Hóu, and V. Muthukkumarasamy, "Level of conceptual interoperability model for blockchain based systems," in *2022 IEEE Crosschain Workshop (ICBC-CROSS)*. IEEE, 2022, pp. 1–7.

[229] R. Ganguly, Y. Xue, A. Jonckheere, P. Ljung, B. Schornstein, B. Bonakdarpour, and M. Herlihy, "Distributed runtime verification of metric temporal properties for cross-chain protocols," in *2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS)*, 2022, pp. 23–33.

[230] C. Giulio, "Before ethereum. the origin and evolution of blockchain oracles." *IEEE Access*, pp. 1–1, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10131932/

[231] K. E. Moujahid. (2022, November) Introducing a low-latency oracle solution for the defi derivatives market. Accessed on 16 October 2023. [Online]. Available: https://blog.chain.link/low-latency-oracle-solution/

[232] R. Yin, Z. Yan, X. Liang, H. Xie, and Z. Wan, "A survey on privacy preservation techniques for blockchain interoperability," *Journal of Systems Architecture*, p. 102892, Apr 2023.

[233] Q. Zhao, Y. Wang, B. Yang, K. Shang, M. Sun, H. Wang, Z. Yang, and X. He, "A comprehensive overview of security vulnerability penetration methods in blockchain cross-chain bridges," *Authorea (Authorea)*, Oct 2023. [Online]. Available: https://www.authorea.com/users/674544/articles/672844-a-comprehensive-overview-of-security-vulnerability-penetration-methods-in-blockchain-cross-chain-bridges

[234] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[235] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2015, pp. 281–310.

[236] ——, "The bitcoin backbone protocol with chains of variable difficulty," in *Annual International Cryptology Conference*. Springer, 2017, pp. 291–323.

[237] R. Pass, L. Seeman, and A. Shelat, "Analysis of the blockchain protocol in asynchronous networks," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2017, pp. 643–673.

[238] W. Y. M. M. Thin, N. Dong, G. Bai, and J. S. Dong, "Formal analysis of a proof-of-stake blockchain," in *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*. IEEE, 2018, pp. 197–200.

[239] M. Graf, R. Küsters, and D. Rausch, "Accountability in a permissioned blockchain: Formal analysis of hyperledger fabric," in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2020, pp. 236–255.

[240] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual international cryptology conference*. Springer, 2017, pp. 357–388.

[241] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[242] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77 894–77 904, 2019.

[243] J. F. Ferreira, P. Cruz, T. Durieux, and R. Abreu, "Smartbugs: A framework to analyze solidity smart contracts," in *Proceedings of the 35th IEEE/ACM international conference on automated software engineering*, 2020, pp. 1349–1352.

[244] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[245] B. Putz and G. Pernul, "Detecting Blockchain Security Threats," in *2020 IEEE International Conference on Blockchain (Blockchain)*, Nov. 2020, pp. 313–320.

[246] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2490–2510, 2020.

[247] L. Zhou, X. Xiong, J. Ernstberger, S. Chaliasos, Z. Wang, Y. Wang, K. Qin, R. Wattenhofer, D. Song, and A. Gervais, "Sok: Decentralized finance (defi) attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 2444–2461.

[248] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, April 22-29, 2017, Proceedings 6*. Springer, 2017, pp. 164–186.

[249] W. Li, J. Bu, X. Li, and X. Chen, "Security analysis of defi: Vulnerabilities, attacks and advances," in *2022 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2022, pp. 488–493.

[250] G. Kelly, B. McKenzie *et al.*, "Security, privacy, and confidentiality issues on the internet," *Journal of Medical Internet Research*, vol. 4, no. 2, p. e861, 2002.

[251] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164 908–164 940, 2019.

[252] E. Androulaki, A. Barger, V. Bortnikov, S. Muralidharan, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Murthy, C. Ferris, G. Laventman, Y. Manevich, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys conference, EuroSys 2018*, vol. 2018-Janua. New York, New York, USA: Association for Computing Machinery, Inc, Apr. 2018, pp. 1–15.

[253] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, "Prisma2020: An r package and shiny app for producing prisma 2020-compliant flow diagrams, with interactivity for optimised digital transparency and open synthesis," *Campbell Systematic Reviews*, vol. 18, no. 2, p. e1230, Jun 2022.

[254] B. Charoenwong and M. Bernardi, "A Decade of Cryptocurrency 'Hacks': 2011 – 2021," Rochester, NY, Oct. 2021. [Online]. Available: https://papers.ssrn.com/abstract=3944435

[255] R. Zhang, R. Xue, and L. Liu, "Security and Privacy on Blockchain," *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, May 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3316481

[256] B. Putz, M. Vielberth, and G. Pernul, "BISCUIT - Blockchain Security Incident Reporting based on Human Observations," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, Aug. 2022, pp. 1–6. [Online]. Available: https://doi.org/10.1145/3538969.3538984

[257] P. Robinson and R. Ramesh, "General purpose atomic crosschain transactions," in *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 2021, pp. 61–68.

[258] E. E. G. Peter Robinson. (2023) Erc 20 bridge security. Accessed on 16 October 2023. [Online]. Available: https://www.youtube.com/watch?v=hGDH6CNuMM0&t=580s

[259] R. Belchior, "DLT interoperability and more 28 — sok: Cross-domain mev," Sep. 2023. [Online]. Available: https://pt.linkedin.com/posts/rafaelpbelchior_blockchain-interoperability-blockdaemon-activity-7058963415154778112-47Ay

[260] "Rekt - ronin network." [Online]. Available: https://rekt.news/ronin-rekt/

[261] R. Behnke, "Explained: The ronin hack (march 2022)," Mar 2022. [Online]. Available: https://www.halborn.com/blog/post/explained-the-ronin-hack-march-2022

[262] "Rekt - poly network." [Online]. Available: https://rekt.news/polynetwork-rekt/

[263] B. A. [@BeosinAlert], "Polynetwork2 have suffered a potential compromise of private keys or a multi-signature service attack. the hacker has exploited forged proofs to initiate withdrawal operations on the cross-chain bridge contracts across multiple chains. an analysis thread," Jul 2023. [Online]. Available: https://twitter.com/BeosinAlert/status/1675708122944483328

[264] "Rekt - poly network - rekt 2." [Online]. Available: https://rekt.news/polynetwork-rekt2/

[265] D. [@dedaub], "Getting to the bottom of the "34 billion" poly network hack with a technical postmortem. tl; dr poly network had a simple 3 of 4 multisig arrangement over 2 years! looking at the final event we found that the private keys to the addresses marked were compromised. https://t.co/y0emjxcyso," Jul 2023. [Online]. Available: https://twitter.com/dedaub/status/1675516729349292032

[266] [Online]. Available: https://www.rekt.news/poly-network-rekt2/

[267] samczsun [@samczsun], "Five hours ago, an attacker stole 2 million bnb ($566m usd) from the binance bridge. during that time, i've been working closely with multiple parties to triage and resolve this issue. here's how it all went down. https://t.co/e0885dc3lw," Oct 2022. [Online]. Available: https://twitter.com/samczsun/status/1578167198203289600

[268] "Rekt - wormhole." [Online]. Available: https://rekt.news/wormhole-rekt/

[269] "Wormhole bridge exploit incident analysis - blog - web3 security leaderboard." [Online]. Available: https://certik.com/resources/blog/1kDYgyBcisoD2EqiBpHE5l-wormhole-bridge-exploit-incident-analysis

[270] "Nomad bridge incident analysis." [Online]. Available: https://www.coinbase.com/blog/nomad-bridge-incident-analysis

[271] Q. [@Quantstamp], "The exact bug that led to the exploit was in commit 46d145, which introduced new logic that was not part of the audit. https://t.co/k00my1sg1u," Aug 2022. [Online]. Available: https://twitter.com/Quantstamp/status/1554348522656256001

[272] "Harmony incident analysis - blog - web3 security leaderboard." [Online]. Available: https://certik.com/resources/blog/2QRuMEEZAWHx0f16kz43uC-harmony-incident-analysis

[273] "Rekt - harmony bridge." [Online]. Available: https://www.rekt.news/harmony-rekt/

[274] Elliptic, "The harmony horizon bridge hack." [Online]. Available: https://www.elliptic.co/hubfs/Harmony%20Horizon%20Bridge%20Hack%20P1%20briefing%20note%20final.pdf

[275] "Rekt - qubit finance." [Online]. Available: https://rekt.news/qubit-rekt/

[276] [Online]. Available: https://thearchitect.notion.site/THORChain-Incident-07-15-7d205f91924e44a5b6499b6df5f6c210

[277] "Rekt - thorchain - rekt 2." [Online]. Available: https://rekt.news/thorchain-rekt/

[278] Lossless, "Thorchain hacks — could they have been prevented?" Aug 2021. [Online]. Available: https://losslessdefi.medium.com/thorchain-hacks-could-they-have-been-prevented-6e4e478d0831

[279] "Rekt - thorchain - rekt 2." [Online]. Available: https://rekt.news/thorchain-rekt2/

[280] R. Behnke, "Explained: The thorchain hack (july 2021)," Jul 2021. [Online]. Available: https://www.halborn.com/blog/post/explained-the-thorchain-hack-july-2021

[281] ChainSwap, "Chainswap exploit 11 july 2021 post-mortem," Jul 2021. [Online]. Available: https://chain-swap.medium.com/chainswap-exploit-11-july-2021-post-mortem-6e4e346e5a32

[282] "Rekt - chainswap." [Online]. Available: https://www.rekt.news/

[283] R. Behnke, "Explained: The pnetwork hack (september 2021)," Oct 2021. [Online]. Available: https://www.halborn.com/blog/post/explained-the-pnetwork-hack-september-2021

[284] p. Team, "pnetwork post mortem: pbtc-on-bsc exploit," Sep 2021. [Online]. Available: https://medium.com/pnetwork/pnetwork-post-mortem-pbtc-on-bsc-exploit-170890c58d5f

[285] M. P. Anyswap), "Anyswap multichain router v3 exploit statement," Jul 2021. [Online]. Available: https://medium.com/multichainorg/anyswap-multichain-router-v3-exploit-statement-6833f1b7e6fb

[286] nick.eth [@nicksdjohnson], "In case you were wondering if anyswap is safe now they've patched the bug, i present for your consideration, the patch: https://t.co/c3fiawxi4l." [Online]. Available: https://twitter.com/nicksdjohnson/status/1414512086672052238

[287] M. [@MultichainOrg], "1. on may 21, 2023, multichain ceo zhaojun was taken away by the chinese police from his home and has. . . ," Jul 2023. [Online]. Available: https://twitter.com/MultichainOrg/status/1679768407628185600

[288] E. Gkritsi, "$139m bxh exchange hack was the result of leaked admin key," Nov 2021. [Online]. Available: https://www.coindesk.com/tech/2021/11/01/139m-bxh-exchange-hack-was-the-result-of-leaked-admin-key/

[289] R. Behnke, "Explained: The bxh exchange hack (october 2021)," Nov 2021. [Online]. Available: https://www.halborn.com/blog/post/explained-the-bxh-exchange-hack-october-2021

Appendix A. Cross-Chain Concept Formalization

A transaction t is considered final in a ledger l according to a security parameter λ of that network (e.g., the block containing the transaction has a minimum height), and is represented as $final^{l}(t) \rightarrow \{0, 1\}$.

A local transaction yields a state change in the form of a key-value pair. The execution of local transactions emits events. Events act as labels or wrappers for state changes caused by local transactions.

Definition 9 (Cross-Chain Event)**.** *A ccevent gives a cross-chain meaning to a local event. It extends a local event with metadata, representing a state change in a certain ledger. We denote $e^{l \in \mathcal{L}}_{type}(t)$ a cross-chain event that represents a state change of type type against t.target, in domain l, emitted by transaction t, such that $final^{l}(t) = 1$.*

In our model, a *ccevent* is only created when the transaction that emits the corresponding local event is considered final. However, it might be valid or not according to $\mathcal{R}$ that defines the expected behaviour.

Definition 10 (Valid Cross-Chain Event)**.** *A cross-chain event $e^{l_1 \in \mathcal{L}}_{type}(t)$ is deemed valid if and only if it follows the defined cross-chain rules related to it.*

Note that the validity of an event emitted by a local transaction does not imply the validity of the corresponding cross-chain event because the latter might not comply with the defined cross-chain rules.

Formally, a *cctx* is then a composition of n ordered cross-chain events $\mathcal{E}$ across multiple ledgers $\mathcal{L}$ with the same $cctxid$, such that $\mathcal{E} = \{e^{l_1 \in \mathcal{L}}_{type_1}(t_1), e^{l_2 \in \mathcal{L}}_{type_2}(t_2), ..., e^{l_k \in \mathcal{L}}_{type_n}(t_i)\}$. The validity of a cross-chain transaction is given by the conjunction of the validity of every cross-chain event in $\mathcal{E}$, that is evaluated against a set of rules $\mathcal{R}$. We consider blockchain rules $\mathcal{R}$ to be a composition of predicates $\zeta = \{\zeta_1(\mathcal{E}), \zeta_2(\mathcal{E}), ..., \zeta_n(\mathcal{E})\}$ over a set of events $\mathcal{E}$.

Appendix B. SoK Methodology

In this section, we present further details on our systematic survey methodology. Figure 2 presents the PRISMA diagram [253] for our survey.

We conducted a systematic literature review by crawling papers using Google Scholar's keyword search. The search was limited to papers since 2015 due to the limited amount of research available before that period. The following search query was used to search for papers within our research scope:

```
("blockchain interoperability" OR "cross-chain") AND
("attack" OR "incident" OR "hack" OR "leaks") AND (
("security" AND ("vulnerability" OR "mitigation"))
OR "privacy")
```

Blockchain interoperability research has been rapidly evolving in the last couple of years. Yet, academic and peer-reviewed work alone falls short of delivering the most up-to-date facts on interoperability, particularly in the analysis of cross-chain hacks. We pay attention to a significant amount of material available as grey literature in online databases such as *Rekt* and *Slowmist*, and online audit reports by reputed companies in the area such as *Certik*, *Chainsecurity*, *Consensys*, *Halborn* and *Trail of Bits*. We also find that many incident reports are divulged through unstructured and informal means of communication, namely blog or social media posts [254]. We strive to uphold the integrity of the findings presented in this work, diligently cross-referencing information whenever possible. Therefore, to the best of our knowledge, the material presented is the most reliable and up-to-date.

To mitigate the potential for unsoundness or bias due to the reliance on gray literature, we meticulously compile data from several sources, and each resource undergoes thorough examination and assessment by at least two paper authors. Additionally, we acknowledge that our analysis of industry solutions and associated vulnerabilities may not encompass the entirety of the landscape, primarily due to limitations in the available documentation. Nevertheless, we make diligent efforts to compile all accessible information concerning projects that collectively represent over 75% of the Total Value Locked (TVL) in cross-chain solutions [32].

Appendix C. Confidentiality as a requirement for Cross-Chain Unlinkability

From our research, we show that the degree of linkability, and consequently anonymity, yielded by an interoperability solution is tied to the capacity to keep local transactions' content confidential. This idea is also supported by [255]. We study the requirements for cross-chain unlinkability to be achieved and propose Lemma C.1, which is proved below. We denote *confidential systems* as $\mathcal{C}$ and *non-confidential systems* as $\mathcal{S}$. Confidential systems are either private blockchains (e.g., Hyperledger Fabric, Quorum,

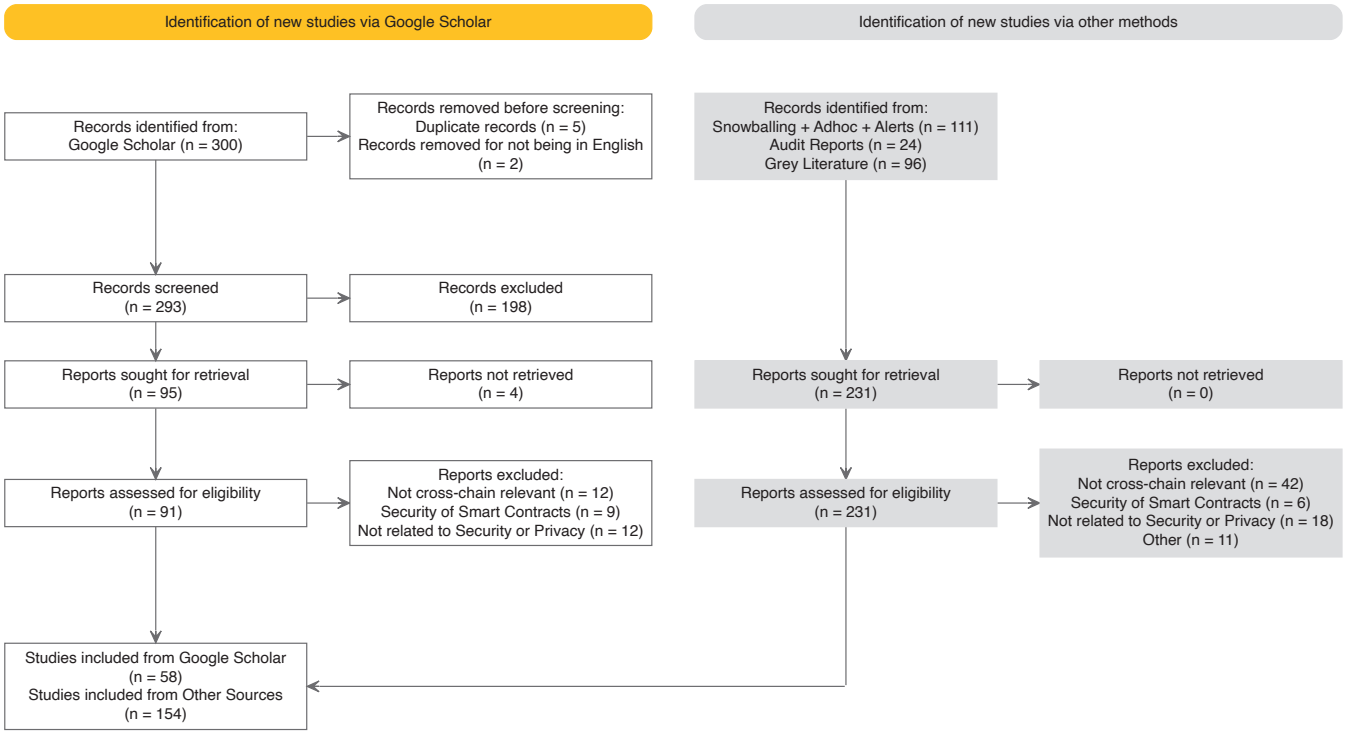

Figure 2. PRISMA Diagram depicting our methodology [253]

DAML's Canton) or public blockchains that are hardened by a privacy-preserving mechanism that hides transactional data (e.g., ZCash, Monero). Non-confidential systems are typical layer-one blockchains with no concern over privacy (e.g., Ethereum, NEAR). We denote an interoperation process (e.g., asset transfer/data transfer) by $\rightarrow$.

Lemma C.1. *Cross-chain unlinkability is unlikely to be achieved without confidentiality on the underlying chains.*

Proof. Interoperability inherently relies on linkability between transactions on a source and target blockchain. However, one must consider that this linkability is undesirable for general users, as it compromises the degree of privacy yielded by the protocol. We identify a direct relation between the confidentiality guarantees offered by one blockchain and the cross-chain anonymity and unlinkability offered by interoperability solutions built on top of these. Table 8 summarizes the comparison based on the privacy guarantees of the privacy guarantees of the ledgers, which is further explained below.

$\mathcal{S} \rightarrow \mathcal{C}$: On the source chain, transaction data (such as the amount, sender, and recipient) is open to everyone. However, since the destination chain is private or has privacy-preserving primitives, only authorized parties can see and link a transaction to the one issued on the source chain. To issue transactions on a permissioned network, there must be a trusted and identified IM with access to the ledger and, optionally, to private channels. Assuming this third party does not disclose information external parties cannot link transactions across chains. Cross-chain unlinkability is guaranteed.

TABLE 8. MAXIMUM ACHIEVABLE CROSS-CHAIN ANONYMITY BASED ON THE CROSS-CHAIN UNLINKABILITY, WHICH IS DEPENDENT ON THE CONFIDENTIALITY OF THE UNDERLYING CHAINS

Source Chain	Target Chain	Max. Unlinkability Achievable	Max. Anonymity Achievable
$\mathcal{S}$	$\mathcal{S}$	CC Linkability	CC Pseudonymity
$\mathcal{C}$	$\mathcal{S}$	CC Unlinkability	CC Anonymity
$\mathcal{S}$	$\mathcal{C}$	CC Unlinkability	CC Anonymity
$\mathcal{C}$	$\mathcal{C}$	CC Unlinkability	CC Anonymity

$\mathcal{C} \rightarrow \mathcal{S}$: The key challenge in this setting is for an action that occurred in the source chain to be validated externally. The two options are a light client in the target chain, where the user presents a way of decrypting source blockchain data, or an interoperability mechanism that has access to the source chain and acts as a trusted party. In the former, an option might be the usage of zero-knowledge proofs, which can be verified while maintaining data confidentiality. In the latter, linkability is possible only if the trusted IM discloses information. A trusted IM can access this information, verify its validity, and issue transactions on the public chain accordingly. Since the IM must be trusted [3], there is cross-chain unlinkability.

$\mathcal{C} \rightarrow \mathcal{C}$: Assuming both blockchains are confidential, only authorized parties can link transactions, including a

trusted IM with access credentials on both the source and target chain. Applying the same logic above, an external observer cannot link transactions in each chain.

$\mathcal{S} \rightarrow \mathcal{S}$: The analysis of various heuristics, such as transaction amounts, addresses, or shared secrets, can enable linking transactions across multiple chains [65], [77]. Mixing services (cf. Section 3.5.1) help cover traces and break transaction linkability. In an ideal setting, these systems achieve their goals perfectly. However, in the real world, these have been studied and are shown not to be effective [126]. □

Interoperability requires a trusted party [3]. In centralized settings, the trusted party can hold records of transactions and corresponding mappings. Therefore, privacy concerns may arise, such as the leakage of private information or, in the worst-case scenario, sold [20]. With a trusted centralized entity that removes outdated records and does not keep track of transactions, there is unlinkability without the risk of being compromised. Cryptographic methods, such as blind signatures, might be a safeguard. We derive a direct consequence from the above Lemma C.1: since cross-chain anonymity depends on the unlinkability of $cctxs$, we extend our initial thoughts in Lemma C.2.

Lemma C.2. *Cross-chain anonymity is unlikely to be achieved without confidentiality on the underlying chains.*

Proof. Cross-chain anonymity is driven by cross-chain unlinkability, and cross-chain unlinkability is unlikely to be achieved without the confidentiality of the underlying chains. Therefore, cross-chain anonymity is unlikely to be achieved without confidentiality on the underlying chains due to the incapacity to provide cross-chain unlinkability under those conditions. □

We derive the main consequence of the above ideas in Corollary C.2.1.

Corollary C.2.1. *The privacy level offered by the interoperability solution is upper-bounded by the intersection of the privacy levels of the underlying chains.*

Appendix D. Future Research Directions

In this section, we delve deeper into the future research outlined in Section 4.4.

D.1. Monitoring in Cross-Chain Systems

Given the inherent vulnerabilities in software systems, enhancing the robustness of cross-chain solutions becomes paramount. Initial efforts should focus on the formal verification of cross-chain protocols using an array of tools to augment the likelihood of their correctness. Concurrently, establishing rigorous security and engineering practices for both on-chain and off-chain components is essential. This includes the implementation of automated tests and the meticulous security scrutiny of software dependencies. Proactive prevention can be achieved through the continuous monitoring of all components. Although the Hephaestus framework presents an intriguing direction [153], empirical benchmarks in real-world contexts remain an essential avenue for exploration. Studying and enhancing UX and UI practices for detecting and reporting attacks is also relevant, to increase the transparency, process, and integrity of attack/vulnerability disclosure. Although some preliminary work is done in this area [210], [256], specific solutions deployed at scale are still missing.

Note that automated frameworks for vulnerability finding often have a high degree of false positives. Additionally, the tendency for contracts to become larger and more complex is exacerbated by the newly cross-chain smart contract paradigm, which will lead to new, complex, hard-to-debug vulnerabilities. These are expressed either as native cross-chain smart contracts [68], by the orchestration of smart contracts across chains [55], or by cross-chain contract calls [257]. We foresee that the market will need cybersecurity professionals with skills in several blockchains, programming languages, and attacks to protect systems from these vulnerabilities.

D.2. Frameworks for Incident Response in Cross-Chain Contexts

Software platforms interfacing with the internet, especially those governing sensitive tasks like cross-chain bridges, necessitate dedicated cybersecurity oversight. The current research landscape underscores the need for enhanced operational security. Preliminary metrics for detecting bridge discrepancies exist [258], yet manual or automated responses each present their challenges. Mistaken detections, for instance, can result in bridge suspensions, impacting user experience and revenue. To date, comprehensive incident response frameworks for generic cross-chain systems remain largely uncharted, despite some industry-specific endeavors.

D.3. Cross-chain Privacy in Heterogeneous Systems

Our findings suggest that cross-chain privacy is predominantly maintained within underlying chains that inherently support privacy-enhancing features. The development and exploration of techniques to ensure unlinkability and anonymity across diverse ledgers remain areas of underexplored research within the scientific community.

D.4. Blockchain interoperability design patterns

Design patterns serve as structured frameworks, enabling developers to craft secure solutions with augmented efficacy. Although each interoperability context possesses distinct characteristics, discerning common challenges and pitfalls inherent to specific interoperability solutions can yield invaluable insights. While blockchain design patterns have undergone rigorous scrutiny, a comprehensive examination of

design patterns across multifarious blockchain applications remains nascent in the current research landscape, reflecting the evolving nature of this domain.

D.5. Data models for blockchain interoperability

Data models are fundamental to interoperability, streamlining complex mappings and varied data formats. Abstract models facilitate a semantic perspective for developers, mirroring the role of SDKs in emphasizing business logic over implementation nuances. Notable strides towards a universal data model are evident through ERC-5164, the ISO model (as adopted by Overledger [224]), SATP Gateways [44], and IBC [225]. However, the path to full standardization remains under exploration, with multiple standards emerging concurrently. The preference for open standards is evident and is crucial for achieving technical interoperability. The importance of this is underscored by initiatives such as BUNGEE [43].

D.6. Empirical Investigations

The research landscape reveals a notable gap in empirical studies addressing the detection of theoretical attacks and associated mitigation strategies identified in our analysis. Additionally, there seems to be a scarcity of in-depth examinations focusing on specific IMs. A couple of research trajectories stand out in terms of their pertinence and potential impact. Firstly, the identification of cross-chain Miner Extractable Value (MEV) is becoming increasingly salient due to the rapid expansion of blockchain bridges, coupled with substantial investments to enhance their usability and facilitate the onboarding of newcomers. Secondly, the empirical exploration of oracle manipulation within the cross-chain context [65], [226], [259] presents a promising direction for future investigations.

Summary

The importance of comprehensive security in cross-chain operations cannot be understated. Despite the extensive research conducted on cross-chain security, ensuring protection across the entire stack remains imperative. Given the vast attack surface, solely relying on preventive measures, such as continuous monitoring and proactive security, is insufficient [153]. We strongly recommend practitioners bolster their defenses by integrating reactive security measures, including robust incident response frameworks.

Regarding privacy, current research appears to be relatively underexplored. However, as interoperable central bank digital currencies gain traction – evidenced by references like [95], [227] – we foresee a more substantial impetus driving advancements in cross-chain privacy solutions. We envision that protocols filling this gap will emerge especially with the recent evolution of zero-knowledge technology, according to our findings. We also highlight the importance of researching how privacy can be guaranteed in regulated and auditable environments.

TABLE 9. DATASET OF CROSS-CHAIN BRIDGE HACKS ORDERED BY DATE

Bridge Name	Hack Date	Amount (Million USD)
Thorchain	June 2021	0.14
Thorchain	July 2021	5.00
Thorchain	July 2021	8.00
Thorchain	July 2021	0.08
Chainswap	July 2021	4.40
Chainswap	July 2021	0.80
Anyswap	July 2021	8.00
Poly Network	July 2021	4.40
Poly Network	August 2021	611.00
pNetwork	September 2021	13.00
BXH	October 2021	139.00
Nerve	November 2021	0.54
Multichain	January 2022	3.00
Qubit	January 2022	80.00
Wormhole	February 2022	326.00
Meter	February 2022	7.70
Ronin	March 2022	624.00
Harmony	June 2022	100.00
Nomad	August 2022	190.00
CelerNetwork	August 2022	0.24
BNB	October 2022	566.00
QANplatform	October 2022	2.00
Rubic	November 2022	1.20
pNetwork	November 2022	10.80
Rubic	December 2022	1.40
Multichain	February 2023	0.13
Allbridge	April 2023	0.57
Cellframe Network	June 2023	0.07
Multichain	July 2023	130.00
Mixin Network	September 2023	200.00
Orbit Bridge	December 2023	81.88
Socket	January 2024	3.30
	Total	**3238.04**

Appendix E.
Real World Cross-Chain Bridge Hacks

In Table 9 we present the entire dataset of cross-chain bridge hacks since June 2021. Additionally,Table 10 presents a more thorough analysis of each of the 18 hacks studied in Section 4.2.2. We describe the hack in detail, map to our model and present a set of mitigations that can mitigate similar attacks in the future.

TABLE 10. DESCRIPTION AND POSSIBLE MITIGATIONS FOR SOME OF THE MOST PROFITABLE CROSS-CHAIN BRIDGE HACKS.

Bridge & Refs	Mapping to our model?	Description	Mitigations
Ronin Bridge [260], [261]	The validators were compromised. The attackers compromised 5 out of 9 validators – the exact threshold.	• Nobody noticed for 6 days. No monitoring existed. • 5 out of 9 validators were needed to approve transactions, whereas 4 were controlled by the same entity Sky Mavis. • The Axie DAO controlled the 5th validator, however, there was a gas-free RPC node through which Sky Mavis had access to the Axie DAO validator.	• $\mathcal{M}_{68}$ – Insert monitoring procedures in the bridge. • $\mathcal{M}_{60}$ – Improve cryptographic key management (e.g., cold wallets, or multi-signatures). • $\mathcal{M}_{61}$ – Increase the number of validators, and the threshold necessary to deem a proof valid. • $\mathcal{M}_{57}$ – Audit not only smart contracts but all the infrastructure that is behind. • $\mathcal{M}_{69}$ – Set withdrawal limits. • $\mathcal{M}_{70}$ – Do not give excessive permission to individual external entities.
PolyBridge [172], [262]	The contract that manages the public keys of active keepers. The user accessed this contract through the bridge one.	• EthCrossChainManager (the bridge contract) has a function executeCrossChainTx() that calls a destination smart contract to unlock tokens passed as an argument. Also, there is a EthCrossChainData contract that manages validators' public keys. • The attacker accessed the function putCurEpochConPubKeyBytes(bytes) that updates the validators' public keys in the EthCrossChainData contract. • Since EthCrossChainManager is the owner of EthCrossChainData, the call would pass the isOwner() check. • Also, to trick the EthCrossChainManager contract to call that function, the attacker relied on his knowledge of the EVM. He found a hash collision where the first four bytes would match the first four bytes of the signature hash of the target function.	• $\mathcal{M}_{52}$ – Smart contracts accessed by users should not have direct access to management smart contracts. • $\mathcal{M}_{71}$ – In dynamic bridges, when receiving a contract address as an argument, check that it represents a contract and, if possible, that the corresponding method being called is valid. • $\mathcal{M}_{69}$ – Set withdrawal limits.
PolyBridge [263]–[266]	Validators' keys were compromised	• 3 out of 4 keys were compromised for a 3 out of 4 multi-sig. • The attacker authorized withdrawals in multiple destination chains	• $\mathcal{M}_{60}$ – Improve cryptographic key management (e.g., cold wallets, or multi-signatures). • $\mathcal{M}_{61}$ – Increase the number of validators, and the threshold necessary to deem a proof valid.
BNB Bridge [173], [267]	Buggy proof verification mechanism.	• The Cosmos' IAVL proof.go implementation had a bug when checking the validity of the proof on the target chain.	• $\mathcal{M}_{51}$ – Make sure third party components/libraries have been audited by multiple entities. • $\mathcal{M}_{68}$ – Freeze deposits and withdrawals to and from the bridge.
Wormhole [268], [269]	A bug was introduced in the proof verification component in the target chain.	• The bridge relies on a set of 19 guardians. • Guardians sign events emitted on both chains. • Due to a mistake, the version solana program being used didn't verify correctly the signatures. • The attack happened a few hours after a patch was fixed in GitHub.	• $\mathcal{M}_{72}$ – Do not publish (push) critical fixes before those changes are deployed. • $\mathcal{M}_{38}$ – Perform security audits with the different versions of the libraries being used. • $\mathcal{M}_{69}$ – More than 93,000 ETH was moved back to Ethereum which could have been avoided if transfers were paused/blocked
Nomad Bridge [170], [270], [271]	The verification of the lock proof would deem every message valid.	• The contract was initialized with 0x0 as a trusted root. • If calling directly the *process()* function in the Replica contract (the bridge smart contract in each chain), it would internally call the *acceptableRoot()* function with the result of *messages[_messageHash]*. • If a message was invalid, i.e., was not yet proved, *messages[_messageHash]* would return 0x0, calling the *acceptableRoot()* function with 0x0 as a parameter. Given that 0x0 was set as a trusted root, the validation would be successful.	• $\mathcal{M}_{73}$ – A bug was introduced shortly after an audit by an external team. Changes in critical components of the code should not be done after an audit.
Harmony [272]–[274]	Validators' keys were compromised	• The bridge relied on a 2 out of 5 multi-signature and two addresses in a hot wallet were compromised. • Harmony stopped the Horizon bridge to prevent further transactions, however, the attacker was able to swap funds to ETH in the Ethereum blockchain.	• $\mathcal{M}_{60}$ – Improve cryptographic key management (e.g., cold wallets, or multi-signatures). • $\mathcal{M}_{61}$ – Increase the number of validators, and the threshold necessary to deem a proof valid.
Qubit Finance [168], [275]	A deprecated function allowed minting tokens without a valid proof.	• Developers forgot to remove a deprecated function from the smart contract that allowed a zero address to call a *safeTransferFrom()*. • The attacker called the deposit function in the source chain (Ethereum) passing an invalid token. The transaction did not revert and the smart contract in the destination chain was instructed to mint xETH tokens to the attacker's address on BSC.	• $\mathcal{M}_{59}$ – Automatic tools allow identifying deprecated (or unused) functions. • $\mathcal{M}_{55}$ – Code reviews should suffice to mitigate this vulnerability.
Meter [169]	Implementation bug in the deposit function in the contract deployed to the source chain.	• The implementation was a modified version of Chainsafe's ChainBridge. They added a new function to deal with native tokens. • The attacker exploited the existing *deposit()* function. The handler (called from the *deposit()* function) had a faulty condition to check for wrapped assets which assumed tokens were already transferred by the bridge. The attacker could pass an arbitrary amount of funds that were transferred to the attacker's address.	• $\mathcal{M}_{74}$ – Know and understand thoroughly a codebase before forking it, especially before creating new functionality. • $\mathcal{M}_{51}$ – Audit code before and after changing code.
Thorchain #1 [171]	Locking a token with a name similar to ETH was interpreted as valid ETH.	• Logical bug in the Ethereum Bifröst smart contract caused fake tokens named "ETH" to be interpreted as real ETH.	• $\mathcal{M}_{12}$ – Whitelisting valid token contracts.
Thorchain #2 [276], [277]	Implementation bug in the relayer. The attacker pretended to transfer funds, taking advantage of the deposit verification mechanism.	• The hacker wrapped the router with a specific smart contract implementation that tricked the bridge smart contract. • They were able to trick the bridge smart contract into processing *msg.value* tokens, even if 0 was provided. • The vulnerability was already known (there was also a comment in the code pointing to the affected loop)	• $\mathcal{M}_{75}$ – Fix bugs as soon as they are detected. • $\mathcal{M}_{68}$ – This attack was performed using multiple transfers, thus, a limit could have been set to limit the number of transfers – e.g., per user, per day, or both.
Thorchain #3 [278]–[280]	The user forged an event deposit. Convinced the bridge that a certain action took place.	• The attacker noticed that if a deposit event was sent to the bridge smart contract the *returnVaultAssets()* function would return the "deposited" ETH to the sender. • The attacker deployed a fake contract, emitted a false event and sent it to the function, which returned real ETH to the attacker	• $\mathcal{M}_{12}$ – Whitelisting valid token contracts.
Chainswap [281], [282]	Access to critical infrastructure allowed whitelisting attacker addresses.	• On Ethereum, the attacker was able to exploit the proxy factory contract, minting tokens directly into different addresses. • There was a bug in the token cross-chain quota code. The signature node automatically increases the on-chain swap bridge quota. However, a logical code flaw allowed addresses that weren't whitelisted to automatically increase this amount.	• $\mathcal{M}_{51}$ – Smart contract auditing to identify vulnerabilities – in this case in the signature verification procedure.
pNetwork [283], [284]	The attacker emitted fake token burn events which were accepted by the source chain.	• Attackers stole BTC collateral for the pBTC-on-BSC bridge. • A series of events was created from faulty contracts, with only one being a legit peg-out request. • The attacker produced bridge back requests which were accepted. • On the original side (BTC) did not validate the requests, unlocking the funds to the attacker.	• $\mathcal{M}_{12}$ – Whitelisting valid token contracts. Events from invalid contracts should not be accepted.
Anyswap [285], [286]	The attacker exploited a bug in the signature generation algorithm.	• The attacker reconstructed the V3 router MPC account's private key due to a bug in the implementation of the random value generation algorithm. • Two transactions used the same (supposedly) random value to generate a signature which compromised the private key	• $\mathcal{M}_{76}$ – Follow standard practices, namely RFC 6979
Multichain [175]	The attacker bypassed the signature verification on the target chain.	• The function that originated the attack was not being used anywhere, it was dead code. • A fake token contract was understood by the bridge as a Multichain token. • The attacker could bypass the signature verification in the ERC-20 *permit()* function, by supplying a token contract that didn't have the permit() function implemented. This caused the fallback function to run instead of reverting. • Multichain dapp requested from all of its users a practically infinite approval sum to save gas fees, which allowed the user to withdraw practically any funds.	• $\mathcal{M}_{59}$ – Automatic tools allow identifying dead code. • $\mathcal{M}_{12}$ – Whitelisting valid token contracts. • $\mathcal{M}_{53}$ – As a user, do not grant access to all of your tokens when requested by a Dapp just to save transaction fees – coined as the baDAPProve problem
Multichain [27]	The attacker accessed internal off-chain infrastructure	• The details of this hack have not been explained yet. We refer the reader to [287] for further details. • Either a rug pull, an internal hack, or an off-chain infrastructure compromise.	We cannot propose mitigations due to not having the details of the attack
BXH [288], [289]	The private key associated with the bridge smart contract on the destination chain was compromised	• Peckshield and BXH came to the conclusion that the hacker took control over the smart contract deployed at the Binance Smart Chain after getting hold of the administrator's private key • It is suspected that this attack was an inside job using a phishing email.	• $\mathcal{M}_{70}$ – Remove a single point of failure caused by admins (or users) having excessive permissions. • $\mathcal{M}_{32}$ – Inside job attacks can be mitigated using multi-signatures or multi-party computation to decentralize responsibilities.

Appendix F.
Meta-Review

F.1. Summary of Paper

This paper surveys the current state of blockchain interoperability mechanisms in both academia and industry. It classifies their approaches and how they correspond to real-world attacks and vulnerabilities. Each section provides insights and principles for the design of security, privacy, and governance mechanisms of future work.

F.2. Scientific Contributions

- Provides a dataset for public use.

F.3. Reasons for Acceptance

1) The paper provides a well-written and clear survey of the current state of blockchain interoperability mechanisms.
2) The work connects attacks to causes, and shows how to categorize those attacks based on the causes.
3) The authors identify gaps in current research and development trends as well as principles to avoid future pitfalls

F.4. Noteworthy Concerns

1) The insights provided in the paper are very low-level and concern either the low-level structure of existing systems, or low-level suggestions for building future ones. Coupled with the large scale of the tables and density of information, this makes it challenging to extract new high-level takeaways about how to think about the overall security of interoperability mechanisms.
2) Some of the definitions lack a level of formality needed to apply them to specific systems.

Appendix G.
Meta-Review Response

We emphasize that Section 4.3 provides general recommendations for operators of blockchain interoperability systems, offering high-level insights classified into the relevant layers. For example, in 4.3.1, we highlight the ad-hoc design of cross-chain protocols, which increase the attack surface for hackers, the need for monitoring, and continuous integration practices. Similarly, in 4.3.2 and 4.3.3, we highlight high-level aspects that are crucial to the area such as Service Level Agreements (SLA) for operators, attractive bug bounties, and the exposure of code through open-source. Additionally, Section 4.4 outlines Future Research Directions, presenting broader insights into areas of interest within blockchain interoperability, including considerations on monitoring, incident response, standardization bodies, and the potential application of Miner Extractable Value (MEV) as a defense mechanism for cross-chain scenarios. We believe these sections effectively address the need for concise, high-level insights and demonstrate our commitment to providing valuable contributions to the field. Finally, we would like to emphasize that our manuscript includes 17 relevant and concise insights. Each numbered insight encapsulates key findings derived from our extensive research and interpretation of the large tables presented. We have made a big effort to make sure the relevant notations are added to each table to improve readability.