Security and Privacy Challenges in Blockchain Interoperability - A Multivocal Literature Review

Terje Haugum
terhaug@stud.ntnu.no
Norwegian University of Science and Technology
Trondheim, Norway

Bjørnar Hoff
Norwegian University of Science and Technology
Trondheim, Norway
bjohof@stud.ntnu.no

Mohammed Alsadi
Norwegian University of Science and Technology
Trondheim, Norway
mohammed.alsadi@ntnu.no

Jingyue Li
Norwegian University of Science and Technology
Trondheim, Norway
jingyue.li@ntnu.no

ABSTRACT

Blockchain technology has achieved increased interest over the last few years. Transferring data and value across different blockchains is one of the biggest obstacles to further expansion. Blockchain interoperability allows different networks to communicate and transfer data between them and are increasingly crucial for blockchain applications. However, the concern about security and privacy in blockchain interoperability arises naturally. This work aims to provide the state-of-the-art related to security and privacy challenges in blockchain interoperability. We conducted a multivocal literature review (MLR) and analyzed 16 scientific and 30 grey literature, respectively. Our MLR identified security and privacy challenges in interoperable blockchain networks while presenting mitigation regarding these vulnerabilities. We have also identified further research directions to mitigate and prevent future attacks and exploitation.

CCS CONCEPTS

• **Security and privacy → Distributed systems security**.

KEYWORDS

Blockchain, security, privacy, interoperability

ACM Reference Format:
Terje Haugum, Bjørnar Hoff, Mohammed Alsadi, and Jingyue Li. 2022. Security and Privacy Challenges in Blockchain Interoperability - A Multivocal Literature Review. In *Proceedings of Evaluation and Assessment in Software Engineering (EASE '22).* ACM, New York, NY, USA, 8 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Since the introduction of Bitcoin in 2008 [35], Blockchain -as a technology for achieving distributed database of records- has gained tremendous popularity. Blockchain is considered as the next disruptive technology under the umbrella of Industry 4.0, and it has assimilated impacts to the internet [10]. The distributed feature of Blockchain coupled with other distinguishable features such as immutability, transparency, and security has helped the technology to be exploited beyond finance such as Supply Chain Management, electronic voting, IoT and many others. Further, the introduction of smart contracts has brought programability, which allows users/organizations to build their own applications on top of Blockchain. This allows users to complete transactions or data exchange without the need of any centralized and trusted third-party authority [7].

Blockchain has become a crucial player in the Financial Technology (FinTech) industry. According to Research and Market report [1], The Blockchain market size is projected to grow from USD 4.9 billion in 2021 to USD 67.4 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 68.4% during the forecast period. This huge market is attractive for attackers, thus concerns about security and privacy risks arises naturally. For example, in [30], researchers used Oyente [2] tool to analyse 19.366 existing Ethereum smart contracts which have a total balance of about 3,068,654 million Ethers, approximately equivalent to 30 million USD. The results showed that 8.833 contracts are vulnerable to security attacks. Further, in June 2016, a malicious user stole around 60 million US dollar from Ethereum platform caused by a bug in DAO smart contract. This allowed the attacker to recursively drain the DAO of ether collected from the sale of its token [8]. Such cases are barriers which prevent Blockchain technology from reaching it's full potential. To address these challenges, new security approaches and proposals, new Blockchain platforms with new features are introduced.

New blockchains have emerged and grown independently with their own features claiming that its more secure and capable to offer better features than the existing platforms. This translates to a critical point in blockchain technology where the different types of blockchains are restricted to their own set of rules. The increased number of unconnected and independent blockchain systems, causes a big fragmentation in the field of research as the majority of blockchain systems operates within silos [24]. From business perspectives, these Blockchain platforms should be able to

EASE '22, June 13–15, 2022, Goteborg, Sweden

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/XXXXXXX.XXXXXXX

[1] https://www.researchandmarkets.com/reports/5025113/blockchain-market-with-covid-19-impact-analysis

[2] https://github.com/ethereum/oyente

interact with each other in order enhance buisness processes and introduce new add-on values for both users and organisations. However, integration with other systems/Blockchains is a non-trivial challenge primarily due to differences with respect to platforms, consensus mechanism, and governance. Todays software enterprise truly relies on collaboration and interaction, so blockchains that focuses on interoperability has therefore increased in popularity by researchers and industrial partners in recent years.

There exists several studies on the security and privacy challenges of blockchain technology, but a few of them target security and privacy challenges in interoperable blockchain networks. A systematic literature review about blockchain interoperability [48] stated that the limitation of inter-blockchain communication are security, privacy, lack of control, scalability, and not supporting hybrid systems. Motivated by the limitation given by [48], this paper focus on security, privacy and vulnerabilities found in interoperable blockchains.We performed a MLR covering both scientific and grey literature. The former is used to analyze current state-of-art regarding security and privacy issues in interoperable blockchains while the latter is used to help us better understanding these issue due to lack of research in this field. We developed three research questions and build our search term to seek answers to these questions using various resources. A total of 489 scientific papers and 333 grey literature was found. This set was reduced to 16 and 30 in scientific and grey literature respectively after paper filtering. The main contributions of this paper are: 1) identify the main security and privacy vulnerabilities targeting blockchain interoperability, 2)identify mitigations to address these vulnerabilities and 3) higlight the challenges associated with these mitigations.

The structure of the paper is as follows. Section 2 presents related work. In section 3, we describe our research method. Section 4 reports research results and Section 5 discusses the results. We draw conclusions in section 6.

2 RELATED WORK

There are tremendous scientific literature about the blockchain technology and its interoperability in general, with a few focusing on security and privacy aspects. Belcior et.al [4] conducted a survey about blockchain interoperability mapping extant literature and classifying studies in different categories. This survey provides a holistic overview of interoperable blockchains with different challenges, future work and standards. It's highlighted that the open issues towards achieving interoperable blockchains are privacy and security. Similarly, authors in [48] conducted a review gathering scientific research on interoperability among heterogeneous blockchains and observed that studies on security risks related to interoperable blockchains are insufficient. The need for blockchain interoperability and how to manage a paradigm shift where blockchains communicate is discussed in [45]. Even authors provide the current state of the art in cross-chain communication, their work does not focus on identifying security and privacy challenges regarding these protocols. On the other hand, [27] strictly follows the formal definition of interoperability and proves that is impossible for two blockchains to interact with each other. The paper highlights, that relaxing the definition gives the possibility to create a 2-in-1 blockchain with two ledgers. Additionally, a survey of all the available cross-blockchain communication solutions is presented in [39]. This survey categorizes the solutions into four categories, sidechains solutions, blockchain routers, smart contracts, and industrial solutions. Furthermore, it compares these categories and discusses their limitations and weaknesses. Authors in [11] propose a proof of concept framework using smart contracts to provide secure communication between heterogeneous blockchains. The proposed system focuses on how Ethereum blockchain can be used to securely share and transfer healthcare data. The system only supports heterogeneous (public and private) blockchains on the Ethereum platform, and not hybrid systems, such as Bitcoin.

Many surveys or literature reviews, such as [3, 5, 12, 13, 16, 20, 20–22, 29, 34, 51, 53], focus on blockchain's security and privacy. However, none of these targets the security and privacy challenge associated with interoperable blockchains. Although [3] targets blockchain security and privacy and examines the vulnerabilities in various blockchain ecosystems components, the study excludes some vulnerable components related to interoperable blockchains.

3 RESEARCH DESIGN

We aim at summarizing the state-of-the-art of vulnerabilities in existing interoperable blockchain networks and research gaps in the field of related challenges. To attain our research goal, we decided to conduct a MLR [18]. MLR is a form of Systematic Literature Review (SLR) which includes grey literature (GL), while a typical SLR use academic peer-reviewed papers only. Generally, GL is any information (not published in books or scientific papers) produced by the private industry or practitioners that is not controlled by any peer-review or publisher [18]. Given that security and privacy in blockchain interoperability is a relatively unsearched field, including GL in our research is necessary for better understanding of the field and allowing us to combine scientific literature with state of the art, produced by practitioners. In this MLR, we focused on answering the following research questions and followed the process proposed in [18].

- **RQ1**: What are the existing security and privacy challenges related to blockchain interoperability?
- **RQ2**: What are the mitigations?
- **RQ3**: What are the open challanges around the mitigations?

RQ1 aims to identify challenges regarding security and privacy, mentioned by researchers and practitioners, in both grey and scientific literature. **RQ2** seeks to provide a overview of the mitigations in the field, while **RQ3** focusing on which challenges follows these mitigations.

3.1 Search Strategy

Due to lack of research in security and privacy in interoperable blockchains, we had to fine-tune the main search string. So far, the most adapted blockchain interoperability solutions are Polkadot and Cosmos. Hence, we opted to use these blockchains as individual terms for our search string. Further, these blockchain names are used in the previously listed research works. This yielded search results suitable to our needs. In order to create the search string, we derived relevant keywords from the research scope and research questions. Then, we defined the search string using the searching terms shown in Table 1 and their combination as follows.

(X1 **OR** X2 **OR** X3) **AND** (Y1 **OR** Y2) **AND** (Z1 **OR** Z2 **OR** Z3 **OR** Z4)

The selection process used for both scientific and grey literature consists of 4 different stages. In scientific literature the four stages are: **1) Literature search and snowballing**: In this stage the researcher a literature search in both google scholar and Oria [1] (a search engine aggregating research papers from scientific databases, including IEEE Xplore, Springer, ACM Digital library, and Scopus), is performed using the search string. When searching using Google, We limited the results from the search by utilizing its page rank and included the first 8 pages without taking the year of publication into account. Limiting the range of the year of publication will not provide the holistic overview we are in search of. To retrieve grey literature for our research, we applied our search string to Google. Applying the first string (X1∧ Y1 ∧ Z3) resulted in 556 000 results (December 2021). Obviously, we need to rely on Google´s page rank algorithm [28], so limiting our search is necessary. This result in a list of scientific literature. Then, this list is extended using the backward snowballing. **2) Remove duplication:** where duplicates from the generated list are removed. In case of different versions, only the most recent paper will be kept. **3) abstract analysis** where the papers’ abstracts are analyzed to excluded irrelevant articles. **4) deep analysis:** where the literature is further further analyzed to determine whether it will be included or excluded. This is done by a full read through of the papers.

For grey literature, the stages were almost the same except the third stage as grey literature resources have no abstract. For this reason, the introduction together with the title are taken into consideration and analyzed to decide whether they give sufficient information about the content of the specific literature in order to categorize them. In order to maintain the validity of each primary study, a standardized rating approach is used. The goal is to reduce the number of studies regarding their relevance. Since quality assessment for grey literature is more complicated than scientific literature, we followed [18] approach to determine whether a source is valid and free of bias. [18] points out that "there is no one-size-fits-all quality model", so we decided to follow their quality assessment checklist for grey literature, considering the authority of the producer, methodology, objectivity, date, novelty, impact, and outlet type. Table 2 presents a quality assessment checklist with a 3-point Likert scale (yes=1, partly=0.5, no=0) combined with the bare binary decision (true=1, false=0), to assign scores to assessment criteria questions. Based on these scorings, we defined a threshold for inclusion and calculated the average of each score, and finally rejected grey literature sources that were lower than 0.5 with a range from 0 to 1.

The MLR was conducted during the autumn of 2021. Using the aforementioned search strings, we found **489** scientific literature and **333** grey literature for further analysis. After filtering, we identified 16 primary scientific papers and and 30 grey literature. We analyzed the data in these primary studies using thematic analysis to answer our research questions.

4 RESULTS

In this section, we present results of our research questions.

4.1 RQ1: security and privacy challenges

From both scientific and grey literature, most of the vulnerabilities are related to the security aspect of blockchain interoperability. Privacy and security are closely related, but privacy attacks target compromising personal information. After data analysis, we have identified the following vulnerabilities and corresponding attacks for security and privacy:

- Wormhole Attack: The wormhole attack happens when two malicious actors infiltrate the network creating a communication tunnel between them and announcing their short path of transaction handling to the other nodes. This will exclude the other nodes from taking part in the existing transaction, potentially stealing fees intended for the honest actors [31]. Hash Time Lock Contract (HTLC) is vulnerable to this attack as it encompasses no more than two rounds of communication which wormhole takes advantage of [31].
- Collusion Attack [17]: Collusion attacks relate to collaboration between multiple nodes generated by a secret agreement in order to behave maliciously. Side Chains and HTLC are vulnerable to this attack, but notary schemes are not due to their reliance on centralized third parties.
- DoS (Denial of Service) in Atomic Swap Vulnerabilities: Atomic swaps, also known as atomic cross-chain trading, offer a way to swap cryptocurrencies peer-to-peer from different blockchains directly without the requirement for a third party, such as an exchange. Atomic Swap utilizes the strategy of HTLC. Atomic Swap is vulnerable to DoS attack [14]. A malicious party could inevitably lock the assets as the initiator of the swap is in control of the abortion method.
- Loss of fund in Atomic Swap: is a security issue where funds of the parties involved could be lost if they go offline for a longer period than the timeout before the withdrawing execution and after giving their secret [41]. HTLC based interoperability solutions are vulnerable to this attack.
- Double Spending Attack: in interoperable blockchains, this attack occurs when one user has multiple accounts in a network (or are in collusion with multiple accounts). The user can first have a transaction with a user on the other network and receive service from an honest client. Afterwards, he can send the same money again from another account and again receive the service from the honest client as he is in another network unknowing of the double-spending attack [43]. Reliance on third parties in Notary schemes prevents collusion with multiple accounts. Thus Notary schemes are not subject to this attack, but Side Chains and HTLC are vulnerable.
- No transaction finality [26, 44]: Finality is used to guarantee that transactions cannot be altered, reversed or cancelled when the transaction becomes final. The longer time period for finality gives more time for additional checks to be performed and reported to the network. In HTCL, contracts are locked for a specific time, which guarantees to reach a form of finality by the end of this time. Strategies utilizing notary schemes and side chains should address this attack.
- Timing attack: Side Chains are independent blockchains that employ their own consensus models and block parameters

Table 1: Searching terms

X1. Blockchain Interoperability	**Y1.** Privacy	**Z1.** Issue
X2. Polkadot	**Y2.** Security	**Z2.** Attack
X3. Cosmos		**Z3.** Challenge
		Z4. Solution

Table 2: Quality assessment for grey literature [18]

Criteria	Questions	Possible answers
Authority of the producer	Is the publishing organization reputable?	**1:** The organization is reputable **0.5:** The organization is not well known **0:** The organization is unknown
	Is an individual author associated with a reputable organization?	**1:** True **0:** False
	Has the author published other work in the field?	**1:** True **0:** False
	Does the author have expertise in the area?	**1:** Author has expertise in the area **0:** Author has not expertise in the area
Methodology	Does the source have a clearly stated aim?	**1:** True **0:** False
	Does the work cover a specific question?	**1:** Yes **0.5:** Not clear **0:** No
Objectivity	Is the statement in the sources as objective as possible? Or, is the statement a subjective opinion?	**1:** Objective **0.5:** Partially objective **0:** Subjective
	Does the work seem to be balanced in presentation?	**1:** Balanced **0.5:** Partially balanced **0:** Not balanced
	Are the conclusions supported by the data?	**1:** Supported **0.5:** Partially supported **0:** Not supported
Date	Does the item have a clearly stated date?	**1:** Clearly stated date **0:** No date
Position w.r.t. related sources	Have key related GL or formal sources been linked to / discussed?	**1:** True **0:** False
Novelty	Does it enrich or add something unique to the research?	**1:** Enriches our reasearch **0.5:** Partially enriches our research **0:** Does not enrich our research
Outlet type	Outlet measures	- 1st tier GL (measure=1): High outlet control/ High credibility: Books, magazines, theses, government reports, white papers - 2nd tier GL (measure=0.5): Moderate outlet control/ Moderate credibility: Annual reports, news articles, presentations, videos, Q/A sites (such as StackOverflow), Wiki articles - 3rd tier GL (measure=0): Low outlet control/ Low credibility: Blogs, emails, tweets

to enhance transaction processing in terms of time. They can also be used for interoperability. For instance, Loom is a sidechain for developing dApps on Ethereum. In [47], Amritraj Singh et al. introduce the potential issue on Loom where the transaction history is periodically updated on the mainchain, and an old version of the transaction history is therefore located on the sidechain periodically as well. This can make the sidechains vulnerable to timing attacks between the updates where the Side Chain is not updated.

- Incompatible cryptography: An interoperable blockchain network may use different signature algorithms and different hashes. This may cause complexity and transaction challenges as a consequence of more functionality and managing different signature algorithms [50].
- Single Point of Failure: A single point failure could be a critical issue for the use of third-party software and the two-way-peg [47]. The two-way-peg method is a solution for transferring coins from a mainchain to a sidechain. There are different methods of implementing two-way-peg, e.g., centralized and federated. [33] describes different types of solutions for gaining interoperability and emphasizes an issue that most notary scheme solutions build upon the trust of the notary. A notary failure could therefore induce a single point failure.
- Private Key Attacks: Storing private keys is similar to password management in many ways. If they end up in a malicious actor's hands, the system/account with the vulnerable

private key is ultimately in ownership of the malicious actor. Having systems for encryption is therefore extremely important. Nonetheless, even with these types of systems in place, the ultimate job of securely storing the password lies with the users [17].

- Sybil Attack: is an attack where a majority of actors of malicious behaviour could potentially lead to a critical security weakness of any blockchain. This attack is mentioned in many research papers on blockchain in general and is still an essential aspect of blockchain interoperability [6][36].
- Eclipse Attack: Although an attack that requires an artificial environment to manipulate a specific node is rare, it is still possible. Eclipse attack is a type of attack which takes advantage of the distributed feature of Blockchain. Attackers aim to isolate a specific user(s) rather than attacking the whole network [23]. Similar to the sybil attack, the eclipse attack is closely related to general blockchain vulnerability. However, it will be inherited by any interoperable system.
- Denial of Service (DoS): Actively preventing transactions and key transfers, locking assets, or other types of locking in the system is seen as DoS attacks. Such attacks should be mitigated in blockchain interoperability systems as best as possible [6, 14, 25, 41].
- No liveness: In the Adversary Capabilities in Practical Byzantine Fault Tolerance [49], the author reviews Polkadot's GRANDPA BFT protocol and shows mathematically that it can't achieve liveness if the adversary is allowed to reschedule the message delivery order in the underlying networks. [42] highlighted that liveness cannot be achieved with asynchronous communication protocols due to the unset response time of the communicating parties.
- Fraud-Proof Attack: Recently, several proof-based attempts at solving Ethereum's scalability problem have been introduced. In [41], an issue with an anchored blockchain on Ethereums sidechain called PLASMA which uses proof of exit and frauds for consensus has been identified. PLASMA does not deal with security where an exit proof has been given, but a malicious actor challenges with a fraud-proof, and the honest actor is offline for the entire challenge period (approximately 7 days). If this happens, the malicious actor could steal the tokens.
- Identifier Leaks in HTLC: is a privacy vulnerability described in [31], in which the payment path holds identifiers from the HTLC that is leaked and could be observed, thus making transaction and involved parties publicly visible [15, 17].

Table 3 provides a comprehensive comparison between the various security and privacy vulnerabilities and attacks, their classification based on whether they target blockchain in general or interoperable blockchains. Further, it matches these vulnerabilities to the different strategies for blockchain interoperability by highlighting the interoperability solutions which are subject to these attacks .

4.2 RQ2: mitigations

As blockchain technology grows, the need for cross-chain communications is essential for further adaption. When connecting both private and public blockchain networks together, it is necessary to do mitigation in order to secure the network and provide the right privacy policies.

Since Cosmos and Polkadot use Proof-of-Stake (PoS), they developed shared security models to share their security across the network and to prevent wealthy attackers from attacking smaller interconnected blockchains with a lower bounded stake. For example, Interchain Security Hub is introduced in Cosmos to share its set of validators with participating (child) chains. Similarly, a shared security model is introduced in Polkadot to define how all parachains connected to the Relay chain can economically benefit from the security provided by their validators [46], hence, providing stronger guarantees for security. Moreover, several mitigations to the security vulnerabilities listed in 4.1 are proposed in the literature.

On the other hand, similar approaches to address the privacy issues related to interoperable blockchains are presented by Cosmos and Polkadot. In Cosmos, Secret Network is introduced as a base-layer blockchain network built using the Cosmos SDK. It is an independent blockchain network that supports smart contracts and data privacy by default, and it is capable of interoperability within the Cosmos network using Interblockchain Communication protocol (IBC). Manta Network is a project on Polkadot aiming for developing a privacy-preserving protocol for the DeFi stack on Polkadot. It offers two smart contract layers, the Decentralized Anonymous Payment (DAP) protocol and the Decentralized Anonymous Exchange (DAX) protocol. DAX is based on zk-SNARK and an automated market maker (AMM), and allows the user to anonymously trade private tokens on the platform [9, 32]. Polkdaot has another on-going project called Phale which aims for building trust in the computation cloud.

Details about mitigation approaches to security and privacy issues is presented in Table 4. It can be noticed that there are vulnerabilities where the primary papers does not provide a proper solution. This could be a result of considering several challenges while providing mitigation to only a few. For instance Malavolta et al. [31] mitigates the issue with the Wormhole Attack in HTLC without having a solution for Denial of Service, asset locking or loss of funds in atomic swaps. From the scientific papers, most of the mitigation to potential vulnerabilities via their own solutions are mostly presented without much consequences. Without further investigation, we cannot reach a conclusion that the proposed mitigation implied further security and privacy challenges.In the grey literature, [50] presents the potential issue of multiple signature algorithms within different networks. Albeit a solution is not proposed, the necessity of handling different algorithms with some form of protocol in order to maintain secure interoperability between blockchains is an important information.

4.3 RQ3: mitigations' challenges

Different vulnerabilities enables the need for further complexity to a system in order to mitigate for those types of vulnerabilities. Here, we present the challenges that arose from the mitigations presented from the primary papers.

Due to blockchain trilemma [19], **scalability** is heavily influenced by the security. From most of the mitigations mentioned

Table 3: Existing security and privacy challenges related to blockchain interoperability.

Vulnerability	Vulnerability Scope		Interoperability Approach		
	General Blockchain	Interoperable Blockchain	Notary	Side Chains/Relay	HTLC
Wormhole attack	✔	✔	✗	✗	✔
Collusion attack	✔	✔	✗	✔	✔
DoS in Atomic Swap	✗	✔	✗	✗	✔
Loss of fund in Atomic Swap	✗	✔	✗	✗	✔
Double Spending Attack	✔	✔	✗	✔	✔
No transaction finality	✔	✔	✔	✔	✗
Timing Attack	✔	✔	✗	✔	✔
Incompatible cryptography	✗	✔	✔	✔	✔
Single point failure	✔	✔	✔	✔	✗
Private key attacks	✔	✔	✔	✔	✔
Sybil Attacks	✔	✔	✔	✔	✔
Eclipse Attack	✔	✔	✔	✔	✔
Denial of Service (DoS)	✔	✔	✔	✔	✔
No Liveness	✔	✔	✔	✔	✔
Fraud-proof attack	✗	✔	✗	✔	✗
Identifier Leaks in HTLC	✗	✔	✗	✗	✔

for research question 2, a decrease in scalability where the overall transaction speed is reduced is a negative outcome from the mitigation itself. Our surveyed studies mentioned that the following mitigation makes the system less scalable.

- Anonymous multi-hop locks with more rounds for solving the issues with HTCL [31].
- Private swaps for solving the identifier leaks inherited by the issue with HTCL [15].
- Mitigation to generate finality by having a wait-time for each transaction described by the developers of Bifrost and Koens et al. [26, 44].
- Implementing a two-way-peg based on simplyfied payment verification [47]. This slows the transactions due to the verification that is needed from both parties.
- The solution of having three observers on each network in order to prevent double spending attacks. This solution was presented by Kuheli Sai and David Tipper [43]. With an increase of nodes, issues, work for the observers, networks etc. will lead to possible scalability-issues.
- In order to improve the security of private keys, the devlopers of Bifrost [44] presented a solution with multiple signatures. This would lead to a slower transaction speed.

A note is that the solution with anonymous multi-hop locks by Malavolta et al.[31] tested the transaction speed and found it performing well in comparison to the original HTCL based system.

For an extra added implementation, there is often an extra added **complexity** to the blockchain system that could generate issues for implementation, updates and further expanding the blockchain. In the mitigations for improving the security of private keys by implementing elliptic curve diffie-hellman presented by [25] and [31], generates a complexity to the system. The same issue is derived by preventing collusion in HTCL-schemes by implementing another layer on top of the interledger protocol [25] as well as the solution to the double spending attack presented by [43].

5 DISCUSSION

Based on the selection and analysis result, it's clear that there is a lack of research being done in security and privacy regarding blockchain interoperability. Related studies, such as [4, 42, 52], focused on interoperability solutions in general. To the best of our knowledge, no MLRs exist on security and privacy issues within blockchain interoperability and the corresponding mitigation. Therefore it was not possible to take inspiration from previous works other than from MLRs focusing on other types of research. Our MLR provides a list of specific vulnerabilities within different types of systems. Some of these systems are used by blockchains in order to induce interoperability between blockchains. However, there are other vulnerabilities which is not covered in our work such as Code Exploitation in smart contracts.

Mitigations: after analysing proposed mitigations for potential security and privacy challenges within blockchain interoperability, we found that the grey literature provided no real descriptive work. This is mainly due to the fact that forum posts, blogs and websites necessarily did not provide a solution to their presented issues. Within the scientific literature, we found that the issue with asset locking using HTCL was not specifically described with a solution. Moreover, most of the solutions to other challenges were not reaching a complete mitigation, meaning they did not provide 100% secure solutions. For instance, the solution to collusion attack on the Interledger Protocol (ILP) where Khosla et al. implemented a layer on top of the ILP. This made it significant harder to collaborate, however, not impossible [25].

Mitigations' challenges: Our goal was to present the challenges arising from the mitigations. The pool of grey literature did not provide any information about these challenges, but it highlights that security and privacy are two important topics for further research and development, in order to create well-regulated blockchain networks. Existing blockchain interoperability solutions, such as Polkadot and Cosmos, constantly improve their security and

Table 4: Link between vulnerabilities from RQ1 and mitigation from RQ2.

Attacks and vulnerabilities	Mitigation(s)	Reference(s)
Wormhole attack	Anonymous multi-hop locks (AMHL)	[31]
Collusion attack	Additional communication layer. Exmaple with CEPA-layer on top of Interledger Protocol	[25]
Denial of Service (DoS) in Atomic Swap		
Loss of funds in Atomic Swap		
Double spending attack	Disincentivizing mechanism with three observers	[43]
	Fee for transactions for all invlolved parties (Cosmos)	[41]
No transaction finality	Implement a wait-time of x	[44][26]
Timing-attack	Anonymous multi-hop locks (AMHL)	[31]
	Additional communication layer, e.g., with CEPA-layer on top of Interledger Protocol	[25]
	Private swaps with the use of secret release	[15]
Incompatible cryptography		
Single point failure	Do not utilize third party software	[36]
	To mitigate single point failure in two-way-peg you could implement simplified payment verification	[47]
	Shared security (Polkadot and Cosmos)	[38][40]
Private key attack	Using a well researched encryption and key exchange algorithm	[44][31][25]
Sybil attack	Make a mathematical alteration to the regular Proof of Stake consensus algorithm in order to make it harder for malicious actors wanting to gain a majority-control. For example Multi-tokens proof of stake (MPoS)	[36]
Eclipse attack	Generate a large routing table able to hold at least some honest nodes	[6]
Denial of Service (DoS)	Presenting a protocol yielding proof of finality and liveness	[49]
No liveness		
Fraud-proof attack		
Identifier leaks in HTLC	Anonymous multi-hop locks (AMHL)	[31]
	Additional communication layer. Exmaple with CEPA-layer on top of Interledger Protocol	[25]
	Private swaps with the use of secret release	[15]

privacy solutions by team members and collaboration [2, 37, 38]. At the time we conduct this review, some features on security and privacy are introduced by the existing interoperability solutions, so the lack of knowledge and research in the field is raised naturally.

In the scientific literature, scalability and complexity are the open challenges around the presented results of our second research question. However, that is challenges outside of the scope of this paper. None of the primary papers imply further implications to security and privacy issues from their own solution to their specific research area. One could say that increasing complexity to a system might lead to security risks. Humans tends to make mistakes, especially doing complicated tasks such as implementing complex systems. This might lead to mistakes in code which in turn could make the system vulnerable to attacks.

6 CONCLUSION AND FUTURE WORK

We performed a MLR on security and privacy challenges in blockchain interoperability. We systematically analyzed 16 scientific literature and 30 informative grey literature. We examined different security and privacy challenges, mitigation, open challenges that arose from the mitigations, and potential future research. By including grey literature in our review, we achieve a broader knowledge base and provide data not found within published literature. In addition, grey literature fosters a balanced and more comprehensive picture. In this MLR, we scrutinized blockchain interoperability in general and existing solutions (Cosmos, Polkadot, etc). By exploring each security and privacy challenges in interoperable blockchains, we have identified several vulnerabilities such as Hash Time Lock Contract, private key attacks, network analysis, and so on. In addition, we have summarized the state-of-the-art mitigation against the identified vulnerabilities and the limitations of the mitigation. In the future, we plan to to evaluate and improve some of the proposed mitigation approaches to address the security and privacy issues of blockchain interoperability.

ACKNOWLEDGMENTS

This work is jointly supported by the National Key Research and Development Program of China (No. 2019YFE0105500) and the Research Council of Norway (No. 309494 and 274816).

REFERENCES

[1] 2022. Oria Search Engine. http://oria.no/

[2] Billy Rennekamp Aditya, Gavin. 2021. Interchain Security. https://github.com/cosmos/gaia/blob/main/docs/interchain-security.md.

[3] Nils Amiet. 2021. Blockchain Vulnerabilities in Practice. *Digital threats (Print)* 2, 2 (2021), 1–7.

[4] Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR)* 54, 8 (2021), 1–41.

[5] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. 2019. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* 7 (2019), 164908–164940.

[6] Jeff Burdges, Alfonso Cevallos, Peter Czaban, Rob Habermeier, Syed Hosseini, Fabio Lama, Handan Kilinç Alper, Ximin Luo, Fatemeh Shirazi, Alistair Stewart, and Gavin Wood. 2020. Overview of Polkadot and its Design Considerations. *CoRR* abs/2005.13456 (2020). https://arxiv.org/abs/2005.13456

[7] Vitalik Buterin. 2013. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper.

[8] Vitalik Buterin. 2016. Critical update re: DAO vulnerability. *Ethereum Blog, June* (2016).

[9] Shumo Chu, Yu Xia, and Zhenfei Zhang. 2021. Manta: a Plug and Play Private DeFi Stack. (2021).

[10] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. 2016. Blockchain technology: Beyond bitcoin. *Applied Innovation* 2, 6-10 (2016), 71.

[11] Gaby G Dagher, Chandra L Adhikari, and Tyler Enderson. 2017. Towards secure interoperability between heterogeneous blockchains using smart contracts. In *Future Technologies Conference (FTC)*. 73–81.

[12] Dipankar Dasgupta, John M Shrein, and Kishor Datta Gupta. 2019. A survey of blockchain from security perspective. *Journal of Banking and Financial Technology* 3, 1 (2019), 1–17.

[13] Francisco José de Haro-Olmo, Ángel Jesús Varela-Vaca, and José Antonio Álvarez-Bermejo. 2020. Blockchain from the perspective of privacy and anonymisation: a systematic literature review. *Sensors* 20, 24 (2020), 7171.

[14] Martijn de Vos, Can Umut Ileri, and Johan Pouwelse. 2021. XChange: A Universal Mechanism for Asset Exchange between Permissioned Blockchains. *World Wide Web* 24 (2021). https://doi.org/10.1007/s11280-021-00870-x https://doi.org/10.1007/s11280-021-00870-x.

[15] Apoorvaa Deshpande and Maurice Herlihy. 2020. Privacy-Preserving Cross-Chain Atomic Swaps. In *Financial Cryptography and Data Security*. Springer International Publishing, Cham, 540–549.

[16] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. 2019. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications* 126 (2019), 45–58.

[17] John Flood and Adrian McCullagh. 2020. Blockchain's future: Can the decentralized blockchain community succeed in creating standards? *The Knowledge Engineering Review* 35 (2020). https://doi.org/10.1017/S0269888920000016

[18] Vahid Garousi, Michael Felderer, and Mika V Mäntylä. 2019. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology* 106 (2019), 101–121.

[19] Seth Gilbert and Nancy Lynch. 2002. Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-Tolerant Web Services. *SIGACT News* 33, 2 (June 2002), 51–59. https://doi.org/10.1145/564585.564601

[20] Harry Halpin and Marta Piekarska. 2017. Introduction to Security and Privacy on the Blockchain. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 1–3.

[21] Huru Hasanova, Ui-jun Baek, Mu-gon Shin, Kyunghee Cho, and Myung-Sup Kim. 2019. A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management* 29, 2 (2019), e2060.

[22] Ryan Henry, Amir Herzberg, and Aniket Kate. 2018. Blockchain access privacy: Challenges and directions. *IEEE Security & Privacy* 16, 4 (2018), 38–45.

[23] Md Rafiqul Islam, Muhammad Mahbubur Rahman, Md Mahmud, Mohammed Ataur Rahman, Muslim Har Sani Mohamad, et al. 2021. A Review on Blockchain Security Issues and Challenges. In *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*. IEEE, 227–232.

[24] Hai Jin, Xiaohai Dai, and Jiang Xiao. 2018. Towards a Novel Architecture for Enabling Interoperability amongst Multiple Blockchains. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. 1203–1211. https://doi.org/10.1109/ICDCS.2018.00120

[25] Akash Khosla, Vedant Saran, and Nick Zoghb. 2018. Techniques for Privacy Over the Interledger. *University of California* (2018).

[26] T. Koens and E. Poll. 2019. Assessing interoperability solutions for distributed ledgers. *Pervasive and Mobile Computing* 59 (2019), 101079. https://doi.org/10.1016/j.pmcj.2019.101079

[27] Pascal Lafourcade and Marius Lombard-Platet. 2020. About blockchain interoperability. *Inform. Process. Lett.* 161 (2020), 105976.

[28] Amy N Langville and Carl D Meyer. 2011. *Google's PageRank and beyond*. Princeton university press.

[29] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2020. A survey on the security of blockchain systems. *Future Generation Computer Systems* 107 (2020), 841–853.

[30] Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. 2016. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 254–269.

[31] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. 2018. Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability. Cryptology ePrint Archive, Report 2018/472. https://ia.cr/2018/472.

[32] Camron Miraftab. 2021. Privacy-Preserving DeFi Stack on Polkadot. *Rarestone* (2 2021), 1. https://rarestone.capital/privacy-preserving-defi-stack-on-polkadot/.

[33] Monika and Rajesh Bhatia. 2020. Interoperability Solutions for Blockchain. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)*. 381–385. https://doi.org/10.1109/ICSTCEE49637.2020.9277054

[34] Joanna Moubarak, Eric Filiol, and Maroun Chamoun. 2018. On blockchain security and relevant attacks. In *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*. IEEE, 1–6.

[35] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.

[36] Yan Pang. 2020. A New Consensus Protocol for Blockchain Interoperability Architecture. *IEEE Access* 8 (2020), 153719–153730. https://doi.org/10.1109/ACCESS.2020.3017549

[37] Polkadot. 2021. Privacy Policy. *Polkadot* (2021), 1. https://polkadot.network/privacy/.

[38] Polkadot. 2021. Security of the network. *Polkadot* (2021), 1. https://wiki.polkadot.network/docs/learn-security.

[39] Ilham A Qasse, Manar Abu Talib, and Qassim Nasir. 2019. Inter blockchain communication: A survey. In *Proceedings of the ArabWIC 6th Annual International Conference Research Track*. 1–6.

[40] Billy Rennekamp. 2021. Interchain Security is Coming to the Cosmos Hub. *Cosmos* (6 2021), 1. https://blog.cosmos.network/interchain-security-is-coming-to-the-cosmos-hub-f144c45fb035.

[41] Peter Robinson. 2020. Consensus for Crosschain Communications. *PegaSys* abs/2004.09494 (04 2020).

[42] Peter Robinson. 2021. Survey of crosschain communications protocols. *Computer Networks* 200 (2021), 108488. https://doi.org/10.1016/j.comnet.2021.108488

[43] Kuheli Sai and David Tipper. 2019. Disincentivizing Double Spend Attacks Across Interoperable Blockchains. In *2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. 36–45. https://doi.org/10.1109/TPS-ISA48467.2019.00014

[44] Eder J. Scheid, Timo Hegnauer, Bruno Rodrigues, and Burkhard Stiller. 2019. Bifröst: a Modular Blockchain Interoperability API. In *2019 IEEE 44th Conference on Local Computer Networks (LCN)*. 332–339. https://doi.org/10.1109/LCN44214.2019.8990860

[45] Stefan Schulte, Marten Sigwart, Philipp Frauenthaler, and Michael Borkowski. 2019. Towards blockchain interoperability. In *International conference on business process management*. Springer, 3–10.

[46] SEQ. 2020. Polkadot — An Early In-Depth Analysis — Part Three— Limitations and Issues. *Seq* (7 2020), 1–3. https://cryptoseq.medium.com/polkadot-an-early-in-depth-analysis-part-three-limitations-and-issues-d8b0a795a3e.

[47] Amritraj Singh, Kelly Click, Reza M. Parizi, Qi Zhang, Ali Dehghantanha, and Kim-Kwang Raymond Choo. 2020. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications* 149 (2020), 102471. https://doi.org/10.1016/j.jnca.2019.102471

[48] Manar Abu Talib, Sohail Abbas, Qassim Nasir, Fatima Dakalbab, Takua Mokhamed, Khawla Hassan, and Khaldoun Senjab. 2021. Interoperability Among Heterogeneous Blockchains: A Systematic Literature Review. *Trust Models for Next-Generation Blockchain Ecosystems* (2021), 135–166.

[49] Yongge Wang. 2021. The Adversary Capabilities in Practical Byzantine Fault Tolerance. In *Security and Trust Management*, Rodrigo Roman and Jianying Zhou (Eds.). Springer International Publishing, Cham, 20–39.

[50] World Bank Group. 2020. BlockchainInteroperability. https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf. Online; accessed 13 December 2021.

[51] Efpraxia Zamani, Ying He, and Matthew Phillips. 2020. On the security risks of the blockchain. *Journal of Computer Information Systems* 60, 6 (2020), 495–506.

[52] Alexei Zamyatin, Mustafa Al-Bassam, Dionysis Zindros, Eleftherios Kokoris-Kogias, Pedro Moreno-Sanchez, Aggelos Kiayias, and William J. Knottenbelt. 2021. SoK: Communication Across Distributed Ledgers. In *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 3–36.

[53] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 52, 3 (2019), 1–34.