Blockchain Interoperability: a Feature-based Classification Framework and Challenges Ahead

Guzmán Llambías[1,2], Laura González[1], Raúl Ruggia[1]
[1]Universidad de la República, Facultad de Ingeniería,Montevideo, Uruguay
[2]Pyxis, Montevideo, Uruguay

{*gllambi,lauragon,ruggia*}*@fing.edu.uy*[1]
guzman.llambias@pyxis.com.uy[2]

Abstract

Blockchain is one of the most recent disrupting technologies. Since Bitcoin emerged as its initial application, many blockchain projects arose offering different features for general and domain specific scenarios. In turn, Blockchain platforms were designed as isolated environments where interoperability was not a native feature. During the last years, academic and industry efforts worked to improve interoperability between blockchain platforms and provided many solutions to solve this problem. However, there is not consensus in the literature on how to classify certain type of solutions and the classification of some of them is not straightforward, which hinders the understanding of the work in the area. In order to organize existing work, this paper provides a feature-based classification framework based on fourteen key interoperability features, that enabled the classification of sixty-two academic papers in three categories and six subcategories. The results show that nowadays research is focused on public interoperability, while private and public-to-private interoperability are still on their first steps. Based on these results, this work also discusses nowadays blockchain interoperability landscape, identifies challenges, and suggests future research directions.

Keywords: Blockchain, interoperability, cross-chain transactions, distributed ledger technologies (DLT).

1 Introduction

In 2008 Bitcoin appeared as a disrupting technology to achieve decentralized payments between peers with zero trust between them [1]. Since then, many other blockchain projects emerged in order to tackle its weakness (e.g. Bitcoin Cash[1], Bitcoin Gold[2], Bitcoin XT[3]), add new features (e.g. Monero[2], ZCash[3]), or expand blockchain original capabilities (e.g. Ethereum [4], Hyperledger Fabric [5], Corda [6], Cardano [7]). Despite these improvements and new features, blockchain platforms tend to work as isolated environments with little to none interaction between each other. Indeed, they focus on immutability, decentralization and reliability and were designed specifically to only trust data generated and managed within the blockchain. Interoperability and system integration were not features provided by blockchain platforms original design, which limit their usage on other use cases. In the last years, some academic and industry efforts were performed in order to achieve interoperability between blockchain platforms [8, 9, 10, 11, 12], which have increased through the years [11].

Blockchain interoperability literature is not straightforward to identify. A primary search covering studies published between 2018 and 2021 on four academic data sources (i.e. IEEE, Springer, ACM and Science Direct) and using the search strings "blockchain AND interoperability" and "blockchain AND cross-chain", returned 800 works which were not all focused on blockchain interoperability. In particular, many works use blockchain as a tool to achieve interoperability between heterogeneous systems on specific domains (e.g. health, internet of things), instead of providing solutions to achieve interoperability between two or more blockchains. First works dated on 2019 have organized the existing literature with quite success

[1]https://bitcoincash.org/
[2]Bitcoin Gold: https://bitcoingold.org/
[3]Bitcoin XT: https://en.bitcoin.it/wiki/Bitcoin_XT

[8, 9]. Unfortunately, these works became quickly outdated as blockchain interoperability fastly evolved. In particular, they include public interoperability solutions (e.g. Notary Scheme, Sidechains/Relays) that focus on cryptocurrency exchange and transfer, which do not cover the current scope of blockchain interoperability [11]. New types of uses cases (e.g. data exchange) and new types of solutions emerged (e.g. Trusted Relays or Blockchain of blockchains) turning these first works to be incomplete with respect to nowadays state-of-the-art. Later works dated on 2021 include new types of solutions and a more updated survey, but they classify the same blockchain interoperability solutions with different categories. As an example, Belchior et al. [11] classifies Cosmos and Polkadot as a Blockchain of blockchain solution, while Lohachab et al. classifies them as a Relay solution [12]. The way in which they arrived to these results is not clear, as they do not specify the classification details in their works. Considering there is not consensus in the literature on how to classify certain type of interoperability solutions, the understanding of the state-of-the-art on blockchain interoperability is currently not straightforward.

The main goal of this paper is to organize existing work related to blockchain interoperability and provide a clear understanding of existing blockchain interoperability solutions, features and definitions. Furthermore, it has the purpose of classifying blockchain interoperability academic studies according to a proposed classification framework, by clearly stating why they were classified that way. Finally, this work aims to identify open issues and challenges in blockchain interoperability as well as directions for future research work.

In order to provide a transparent, reproducible and scientific literature review of blockchain interoperability, this work adopted some features of the PRISMA statement [13] to organize existing work. As a result, sixty-two papers related to blockchain interoperability were selected. This selection allowed to build a feature-based classification framework and key features were identified for each defined blockchain interoperability category. Finally, each paper was analyzed and classified according to the feature-based classification framework into one of six categories: Notary Scheme, Atomic swaps, Sidechain/Relay, Blockchain of blockchains, Gateway, Generic interface and Enterprise Relay. A second level classification categorized these papers according to the blockchain interoperability type: public, private or public-to-private interoperability.

The results of this paper shows that most of the reviewed work focus on public interoperability. These works tackle challenges related to token transfer/exchange, by proposing or improving protocols and solutions. As stated by Belchior et al [11], token exchange is no longer the whole scope of blockchain interoperability. Enterprise organizations started using blockchain technology to improve their business processes and need support for new requirements regarding identity, authorization, consensus protocols, privacy, performance and governance. Related to this, private and public-to-private interoperability are still on their first steps as little work was found. Some work was performed regarding private interoperability, but it tackles specific use case requirements and do not provide a general interoperability solution.

The contributions of this paper include a survey on blockchain interoperability solutions identifying sixty-two relevant papers related to blockchain interoperability dated from January 2018 to May 2021, a feature-based framework with fourteen key features to clearly classify blockchain interoperability solutions, a classification of the surveyed works based on the defined framework and a discussion of nowadays blockchain interoperability landscape, challenges and future research directions.

The rest of this paper is structured as follows. Section 2 presents blockchain and blockchain interoperability concepts. Section 3 presents the research methodology. Section 4 presents the feature based classification framework. Section 5 presents the classification of the surveyed works using the classification framework. Section 6 presents a discussion on blockchain interoperability, challenges identified and future research directions. Finally, Section 7 and Section 8 presents related work and conclusions.

2 Background

This section presents key concepts related to blockchain and blockchain interoperability.

2.1 Blockchain Fundamentals

According to Xu et al. [14] a distributed ledger is a distributed storage across a network of machines that stores transactions in an append-only mode. Once a transaction is registered into the ledger, it cannot be updated nor deleted. These authors also define blockchain as a distributed ledger structured as an ordered linked list of blocks, where each block contains a set of transactions. Each block is linked to its predecessor block by cryptographic hashes that assure the security of the link. The hash of a block is built using the block's data and the hash of the previous block. If a transaction of block n changes, the hash of block n will also change and, as a consequence, the hash of block n+1 cannot be verified as it needs a different hash value of block n. This protection provides users the means to notice if the blockchain was tampered. This behaviour provides in practice, data immutability to the blockchain as tampered blocks will be discarded by

users. The first block of the blockchain is called genesis block. Figure 1 presents a graphical representation of a blockchain.

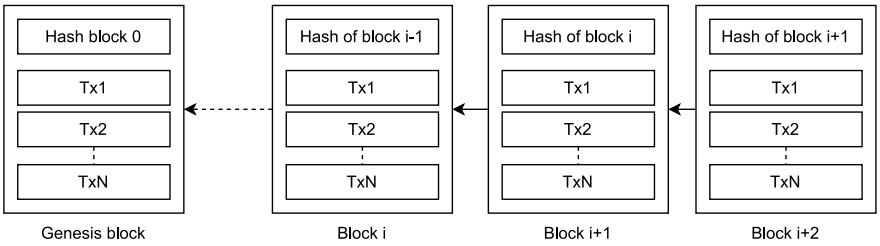

Figure 1: Blockchain structure

Distributed Ledger Technologies (DLT) enables the operation and use of distributed ledgers [15], while blockchain platforms provides the technological layer to operate blockchains [14]. Both provide the software and hardware to run a node and any other software required to have access to the distributed ledger or blockchain network. Hyperledger Fabric, Corda and IOTA[16] are some examples of distributed ledger technologies, while Bitcoin and Ethereum are two examples of blockchain platforms. Bitcoin and Ethereum follow the blockchain structure previously described, while the former use other distributed ledger structures. For example, IOTA uses a Direct Acyclic Graph (DAG) structure[4].

Smart contracts are scripts deployed on the blockchain that are triggered by transactions on an autonomous way by any participant node. They can hold and transfer digital assets or invoke other smart contracts stored on the blockchain. As blockchain computation is based on a closed world assumption, smart contracts can only use data that is stored in the blockchain. In case they need to interact with external systems, they can use Oracles to import external data into the blockchain. Oracles may have many forms. They can be normal users of the blockchain that submit normal transactions with external world data, or they can be components or nodes within the blockchain platform that invoke specific smart contracts to submit this data. With this behaviour Oracles become a trusted third party for the blockchain [14]. Neo Oracle Service[5] and Chainlink[6] are two examples of Oracles.

A blockchain provides the following non-functional properties once a transaction is registered on the ledger: immutability (i.e. once data are registered on the ledger, they cannot be changed or deleted), non-repudiation (i.e. every user must sign the transactions before sending them to the blockchain, which assures the non-repudiation property), and decentralized (i.e. the blockchain storage and execution can be performed by any participant of the network). Other non-functional properties may be available depending on the type of the blockchain. Therefore, blockchains are usually classified into three types: public, private or consortium. In addition, they may be classified as permissioned or permissionless, depending on whether their participants require authorization to participate or not. Public blockchains are traditionally permissionless, while private or consortium blockchains are permissioned. Despite this classification, heterogeneous blockchains arise to cover specific scenarios and some variations to this classifications are present. For example, Monero is a public blockchain relaxing the privacy feature, as well as enabling stealth addressing, unlinkability, untraceability and confidentiality on the transactions amount [2]. Sovrin is another example as it is a public permissioned blockchain, where any participant can read or write transactions but only authorized nodes can operate the blockchain or be validators [17]. Which blockchain platform is more suitable for a specific scenario depends on business requirements and needs [18].

Public blockchains allows users to have full access to the ledger, participate in the consensus protocol and record transactions without restrictions. They have a high level of security (thanks to the consensus protocols, immutability and non-repudiation features), are pseudo-anonymous (participants use a pseudonym instead of their true identity) and no regulation should be followed regarding its use. They are open, can be used by multiple organizations as well as users, and all participants may have a copy of the ledger. Public blockchains focus on decentralized scenarios, where there is no central authority that governs them. Scenarios with a high degree of transparency, immutability of data and free participation are suitable for this kind of blockchains. Bitcoin and Ethereum are two examples of this type of blockchain, whose users may be citizens or private/public organizations.

Private blockchains are closed, used by a single organization and only organization's users have access to the ledger, participate in the consensus protocol or record transactions. Unlike public blockchains, private

[4]We will use DLT and blockchain terms interchangeably in the rest of the paper as they share common characteristics, but they are two different concepts. A blockchain is a DLT but not necessary a DLT is a blockchain.

[5]https://docs.neo.org/docs/en-us/advanced/oracle.html

[6]https://chain.link/

blockchains have a high degree of trust in their participants, who need to be identified in order to participate in the network. The transactions carried out in the blockchain are confidential and not every user may have access. By being governed by a single organization, it is said that this type of blockchain is partially decentralized. This type of blockchain is suitable for scenarios that require a high level of regulation, immutability of data and restricted access to the ledger by users of the organization. Its main focus is to improve internal processes and reduce costs. By running in a trusted environment, they do not require the usage of expensive consensus protocols like public blockchains. This enables them to have better transaction processing at a lower cost. An example of private blockchain usage is Wallmart Canada supply chain management. Wallmart Canada used this technology to improve their supply chain management process and reduce the number of disputes between Wallmart and their carriers regarding discrepancies with their costs. They assured they reduced to 1% the number of invoices with discrepancies and reduced the number of disputes, improving their business processes and costs. In this example, the blockchain users are Wallmart Canada and the carriers.

Finally, Consortium blockchains share many of the characteristics of private blockchains, except that instead of being governed by a single organization, they are governed by a set of organizations that agreed to use the blockchain to reduce costs[7], improve processes[8] or find a solution to business conflicts[9]. Only users of the consortium organizations may have access to the ledger, participate in the consensus protocols or record transactions. Like private blockchains, this type of blockchains has a high degree of trust in its participants, who also need to be identified and authorized to participate. The transactions carried out are confidential and normally only visible to the involved organizations. Organizations only see transactions in which they participate. Unlike private blockchains, this type of blockchain is governed by the consortium, who defines the rules and regulations that organizations must comply with. This type of blockchain is suitable for organizations that want to collaborate in improving their business processes in highly regulated environments, with high levels of confidentiality and data immutability. The consensus protocols used by this type of blockchain ensure high transaction processing at a lower cost (compared to public blockchains). Spunta is an example of blockchain consortium where more than one hundred Italian banks build a consortium and used blockchain technology for reconciliation of bilateral accounts. Blockchain technology allowed automatic interbank reconciliation and detect non-matching transactions using a shared algorithm. In this example blockchain users are a group of Italian banks.

2.2 Blockchain Interoperability

According to Belchior et al. [11], blockchain interoperability involves a source blockchain network that initiates a transaction on its local ledger which must be executed on a target blockchain. However, blockchain interoperability may also refers to business applications that need to communicate with one or more blockchain platforms as well as a blockchain platform that needs to communicate with an external business application.

A cross-chain transaction is a transaction that involves at least two homogeneous blockchain platforms, where a source blockchain sends a message to a target blockchain [11]. Homogeneous blockchains platforms are two or more blockchains that share the same building blocks. A transaction built by these blockchains can be processed by any other homogeneous blockchain. Ethereum, Polygon and BNB Smart Chain are some examples of homogeneous blockchains platforms as they use the Ethereum Virtual Machine (EVM) to execute smart contracts and use the same token structure. BNB Smart Chain token structure defined by Binance standard BEP-20 is an extension of Ethereum token structure defined by Ethereum standard ERC-20. Cosmos zones are another example of homogeneous blockchains [19]. All Cosmos zones built with the Cosmos SDK are built using the same building blocks and sharing the same architecture and structures. Homogeneous blockchains use cross-chain communication protocols to exchange cross-chain transactions [11]. Cross-chain communication protocols are communication protocols that are built based on the blockchain's native building blocks. Polygon's PoS Bridge provides a cross-chain communication protocol that allows cross-chain transactions between Etherum and Polygon.

On the other hand, a cross-blockchain transaction is a transaction that involves at least two heterogeneous blockchain platforms, where a source blockchain sends a message to a target blockchain [11]. Heterogeneous blockchain platforms do not share architecture nor building blocks and are not compatible between each other. Transactions built for a blockchain platform cannot be processed directly by another blockchain platform. Ethereum and Bitcoin are examples of two heterogeneous blockchains. Ethereum has the EVM that allows smart contract processing and uses an account model to allow state changes. In contrast, Bitcoin does not support smart contracts and uses the UTXO model for blockchain transaction processing. Heterogeneous blockchains use cross-blockchain communication protocols to deal with differences in transaction processing

[7] https://www.marcopolonetwork.com/
[8] https://www.r3.com/case-studies/spunta/
[9] https://www.hyperledger.org/learn/publications/dltlabs-case-study

by each blockchain [11]. The Inter Blockchain Communication (IBC) protocol is an example of cross-blockchain communication protocol between Cosmos and Ethereum [20].

2.2.1 Blockchain interoperability types

Blockchain interoperability can be defined according to the involved blockchain types (i.e. public, private) or the systems types that are involved (i.e. business applications, blockchain platforms).

Public interoperability involves the interaction between two public blockchains, which is the focus of current research in the area. The main scenarios involved in this type of interoperability are cryptocurrency exchange, payments (e.g. pay with bitcoin and receive ethers), micro payments with payment channels (e.g. Lightning network [21]) and cryptocurrency transfer (e.g. Zendoo [22]). On the other hand, private interoperability involves the interaction between two private or consortium blockchains. There is currently little research effort in this type of interoperability, where there are some industrial and research examples regarding conflict resolution, data consolidation or supply chain process improvements. Weaver is a platform that enables this type of interoperability [23]. Finally, public to private interoperability involves the interaction between public and private/consortium blockchains and there is also little research in the area. Some examples were presented by Watanabe et al. [24] and Franzoni [25], comprising the payment of services provided by a consortium blockchain. In appendix 1 there are described some industrial interoperability solutions grouped by interoperability type.

On the other hand, system type interoperability involves blockchain platforms and traditional software applications that need to interoperate between each other. System type interoperability is depicted in Figure 2 and is based on the ways of interoperability mentioned by Koens et al. [9]: interoperability between blockchain and legacy systems, interoperability between blockchain platforms and interoperability between two smart contracts on a single blockchain. Platform-to-platform interoperability is defined as the interoperability between two or more blockchain platforms. This type of interoperability involves two blockchain platforms (e.g. Ethereum and Bitcoin) that interoperate at the network layer following the blockchain interoperability architecture presented by Jin et al. [26]. In public interoperability, a source blockchain platform sends a message to a target blockchain platform following one of the operation types described in section 2.2.2 and may involve homogeneous or heterogeneous blockchains platforms. Additionally, public interoperability may involve Value Exchange between Token-based Networks or Data Exchange between Blockchain Business Networks [27]. On the other hand, platform-to-application interoperability is defined by a source blockchain platform that sends messages to a business application following the operation types described in Section 2.2.2. A query to oracles [28] is an example of a query operation, comprising a source blockchain that queries an external system. On the other hand, events provided by some blockchain platforms like Ethereum or Hyperledger Fabric, are examples of command operations, where the blockchain triggers an external action on a business application. Furthermore, application-to-platform interoperability is defined as a source business application that needs to interoperate with two or more blockchain platform. These interactions usually use gateways that provide a generic interfaces like Hyperledger Cactus [29] or Bifröst [30] to achieve these goals. Queries and commands are sent to the gateways that translate request messages to the target blockchain platform format. Some frameworks like Hyperledger Cactus also provide support for coordinated tasks, where the gateway has the role of task coordinator and can provide support for asset exchanges.

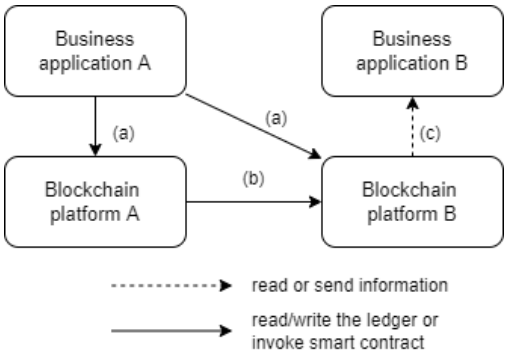

Figure 2: Blockchain interoperability types: (a) A business application needs to interoperate with one or more blockchain platforms; (b) a blockchain platform needs to interoperate with one or more blockchain platforms; (c) a blockchain platform needs to interoperate with one or more business applications.

2.2.2 Blockchain interoperability operations

Blockchain interoperability operations may be of three types, as illustrated in Figure 3: query, command and coordinated operations.

Query operations involves a source blockchain that requests a target blockchain for information of its ledger. The response of this request must have a proof that assures the source that the information is valid

and has passed the consensus protocol of the target blockchain. The source blockchain may use or publish this information on its own ledger with the corresponding proof.

Command operations are one-way operations from a source blockchain to a target blockchain. Command operations include data that need to be sent to the target blockchain with the corresponding proof that has passed the source blokchain consensus protocol. The target blockchain validates the proof and may use or save this information in its ledger. Asset transfer is an example of this type of interaction.

Coordinated operations involve a source and a target blockchain that need to perform some coordinated task between each other and must comply with atomicity and consistency properties of ACID transactions. This type of operation involves an action on the source blockchain, a message sent to the target blockchain and an action on the target blockchain after receiving this message. Target and source blockchain actions must execute atomically and if the target blockchain action fails processing the message, the action at the source blockchain must be rolledbacked. These actions must also guarantee data consistency. Asset exchange is an example of this type of operation.

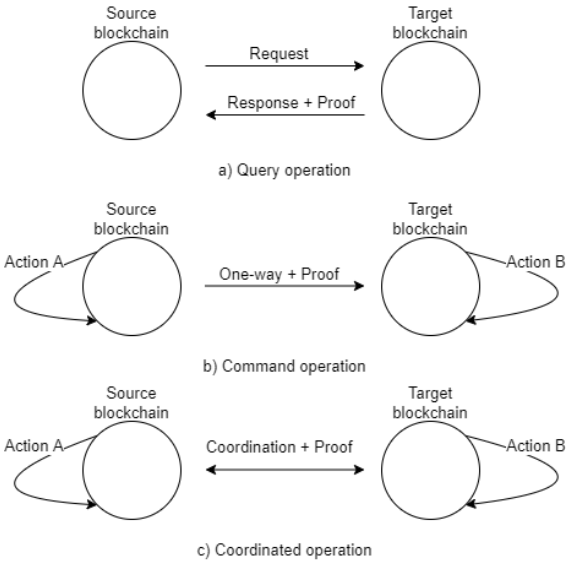

Figure 3: Interoperability operation types

2.2.3 Blockchain Interoperability Motivating Scenario

This section presents a motivating scenario to map the background concepts described in previous sections through a use case example.

The scenario, presented in Figure 4, is based on a simplification of the scenario presented by He et al. [31] and comprises doctors that prescribe medicines to patients, which may use later on to buy medicines on pharmacies. A consortium blockchain is setup comprising hospitals, pharmacies and private clinics as participants, which is used by doctors to issue medical prescriptions. On the other hand, one public blockchain is used by patients and pharmacies to buy their medicines.

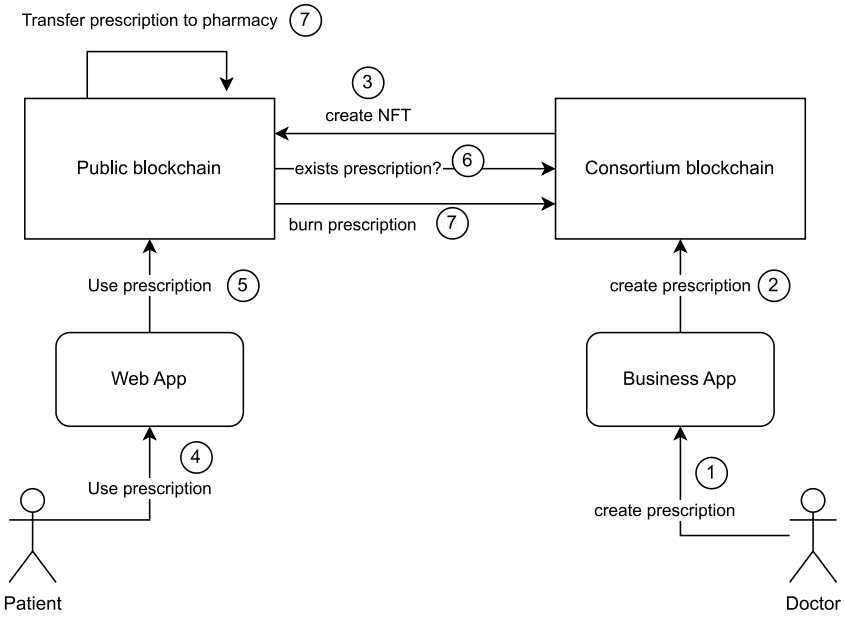

Figure 4: Medical prescription scenario

Doctors use a Business Application to issue a medical prescription that creates a virtual representation of the prescription in the consortium blockchain, with information about the patient, medicine, dosification,

etc. The Business Application creates a blockchain transaction which must be validated by the consensus protocol of the consortium. After the blockchain transaction is validated, the consortium blockchain creates a cross-blockchain transaction to create and assign an non-fungible token (NFT) to the patient on the public blockchain. This NFT only has the hash of the prescription on the consortium blockchain, to keep the patient's data privacy. Information about the patient, medicine or dosification is not present on the NFT.

Patients can buy their medicine on a physical pharmacy office or through their e-commerce using a web site or mobile application. In order to buy their medicine, patients may use another Business Application that may invoke a smart contract on the public blockchain to use the NFT. The public smart contract may create two cross-blockchain transactions on the consortium blockchain: 1) to check the prescription is valid and 2) to mark the prescription as used (burn the prescription). After the prescription is burned, the public smart contract transfers the ownership of the NFT from the patient to the pharmacy for further record management.

Our scenario can be extended with other consortium blockchains owned by other medical institutions or laboratories, that may interoperate with our consortium blockchain to issue medical exams, allowing collaboration with other medical institutions in other cities or countries, following a consortium to consortium interoperability scenario. Also, it can be extended with more public blockchains allowing the purchase of medicine with cryptocurrencies achieving a public to public interoperability scenario. Finally, it can be extended by adding a legacy health system that public and consortium blockchains need to interoperate with in order to fulfill a blockchain transaction.

Our motivating scenario classifies on three of the blockchain interoperability types. It follows a public to private interoperability and includes the two types of System interoperability: 1) platform-to-platform interoperability and 2) application-to-platform interoperability. It also includes the three types of operations: query, command and coordinated tasks. The query operation is used in order to check the prescription is valid (the public blockchain queries the consortium blockchain). The command operation is used between the consortium and public blockchain to create the NFT token after the prescription is created on the consortium blockchain. Finally, a coordinated task can be found when the patient needs to use the prescription. In particular, two tasks need to be coordinated to keep data consistency and atomic commitment: 1) prescription usage on the consortium blockchain, and 2) NFT transfer (step 7 in Figure 4).

3 Research Methodology

This section describes the applied research methodology, which is graphically presented in Figure 5. The first step of the methodology was to review blockchain interoperability literature and identify relevant papers. The result of this step provided the corpus of the academic literature that was used to define and apply the classification framework. The second step was to build an initial version of the classification framework based on existing work. At this step, blockchain interoperability features were identified, defined and grouped together leading to categories (e.g. Notary Scheme). The result of this step provided an initial version of the classification framework with categories and features that define each category. The third step was to examine the papers reviewed on step two and apply the classification framework (defined also in step two) to classify them in one category. In this step, features were identified for each paper in order to classify it. In case the papers could not be classified because there were missing or contradicting features, the process returned to step two to review the classification framework and build a new version. New features were identified or updated and grouped into new or existing categories. As a result, a new version of the classification framework and the process returned to step three. This process iterated until all papers were classified.

To provide a transparent, reproducible and scientific literature review of blockchain interoperability, this work adopted some features of the PRISMA statement [13] to build the survey methodology. Figure 6 shows the steps that were followed: identification, screening, eligibility and inclusion.

The search process selected IEEE, ACM, Springer and Science direct as the main data sources and started using the query string "blockchain AND interoperability". During the eligibility phase, it was noticed that cross-chain transactions is another term for blockchain interoperability, so the following statement was added to the search string: "cross-chain AND blockchain". The final query string was "blockchain AND interoperability OR cross-chain AND blockchain". During the review, referenced works were added by snowball effect or related academic material (e.g. research other relevant articles of a specific author). The search included articles published from January 2018 to May 2021, resulting in 864 potential articles. All articles were retrieved in full text search.

On the screening step, papers were filtered based on title, abstract and keywords examination, keeping only blockchain interoperability related results. In this step many articles were filtered as they used blockchain to achieve interoperability on a specific use case (e.g. health, internet of things, instead of pro-

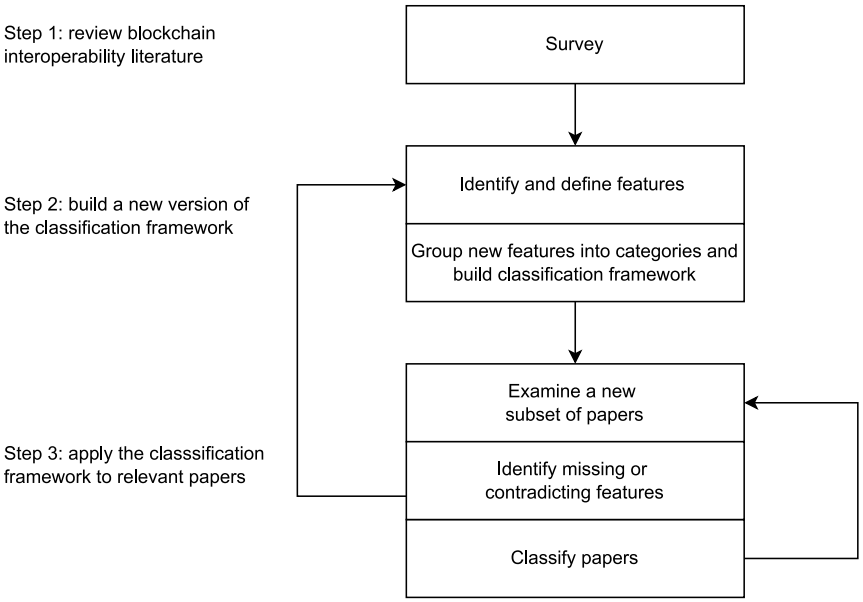

Figure 5: Research methodology

viding solutions to achieve interoperability between two or more blockchains). The result of this step was a selection of eighty-seven relevant papers.

On the eligibility step a full text assessment was performed to discard unrelated articles. This task had a result of fifty six relevant papers. Through this step, six new articles were found out through references and included on the research. The final result of this step were sixty-two papers that become the main data source that guided this work.

4 A Feature-Based Classification Framework

In order to build the classification framework, this work reused and extended the work presented by Belchior et al. [11], which defines three categories of blockchain interoperability solutions: Public Connectors, Hybrid Approaches and Blockchain of blockchains. For the first two categories, the authors also define subcategories. Notary Scheme, Atomic Swaps and Sidechain/Relays are subcategories of Public Connectors, while Trusted Relays, Blockchain Agnostic Protocols and Blockchain Migrators are subcategories of Hybrid Approaches. This work extends Belchior et al. [11] classification to map some solutions that were hard to categorize, as interoperability solutions evolved in its definitions and features. For example, some earlier works are self defined as Sidechain/Relays solutions [32, 33], but nowadays it is more suitable to classify them as Blockchain of blockhains, a new category not available before. On the other hand, newer subcategories like Trusted Relays are not clear enough and became too broad, as they include different level of software complexity on a same category. Simple gateways and complex relays with validators, routing and registry features are all grouped together. Besides this, the existing Trusted relay classification provided by Belchior et al. [11] is sometimes confusing with some works that have a main chain and sidechains [34, 35], features not present in his Trusted Relay definition, but are present on Blockchain of blockchains category. Furthermore, the Trusted Relays definition allows decentralization on trustless environments, contradicting their name. This contradiction was further stated by some of the authors in Ghaemi et al. [36]. Due to all the above mentioned comments, our work extends the original classification to clearly categorize all the reviewed papers. The new classification framework introduces blockchain interoperability features as a main citizen, that enables a classification according to the features each blockchain interoperability solution supports. By applying inference, if a set of features is supported, then the interoperability solutions belongs to a category/subcategory. For example, if an interoperability solution has a main chain, a sidechain with a strong business relationship with the main chain, a relay, a blockchain communication protocol with connectors that adapts messaging format from a source chain to a target chain and a consensus protocol on the main chain to validate sidechains' cross-chain transactions, then the interoperability solution belongs to the sidechain/relay subcategory.

The following subsections presents the features that compose the classification framework.

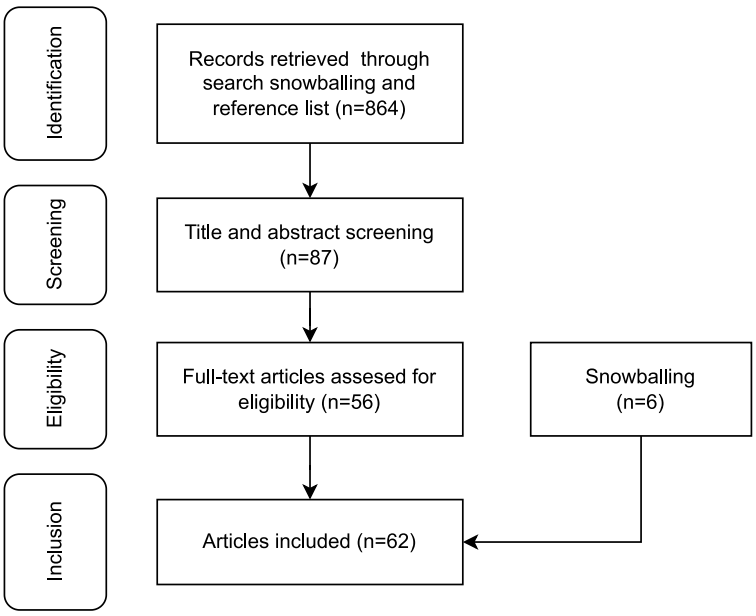

Figure 6: Survey methodology

4.1 Connectors

This feature provides gateway middleware capabilities to the blockchain interoperability solution. Furthermore, it provides a cross-chain communication protocol to connect with homogeneous blockchain platforms or a cross-blockchain communication protocol to connect with heterogeneous blockchain platforms. An interoperability solution may have more than one connector in order to integrate with many blockchain platforms.

4.2 Message adapters

Inspired by the Message Translator pattern from the Enterprise Integration Patterns (EIP) [37], this feature provides data format transformation capabilities to the blockchain interoperability solution. It can be composed with the connector features in order to achieve interoperability between two or more blockchain platforms, in case the blockchains involved use different data formats.

4.3 Router

This is also a feature inspired by the EIP patterns, specifically, the Message Router pattern [37]. It is required when a source system (blockchain or business application) needs to interoperate with multiple blockchain platforms. This feature provides routing capabilities to the interoperability solutions allowing them to route received messages to the corresponding blockchain platform. The Router may have defined the target blockchain location on design time or may be composed with a Registry in order to discover the blockchain location at runtime.

4.4 Registry

This feature is inspired on the service registry pattern for microservices [38] and enables the discovery of relevant resources related to blockchain interoperability, including blockchains, oracles, participating entities, network certificate authorities, smart contracts and ledgers [27]. The registry can be centralized or descentralized as well as be composed with the Router and Connector features to build complex interoperability solutions. As specified by Tam et al. [27], registries can be static (manually predefined), automatically configured or have semantic discovery capabilities.

4.5 Relays

Relays are Simple Payment Verification (SPV) light nodes [1] that validate incoming cross-chain transactions from a source chain, following the source consensus protocol verification rules. Relays' validations follow protocol validation rules like Proof-of-work consensus, Proof-of-Stake or RAFT protocol [39].

4.6 One to one communication

This feature refers to how many blockchain networks are supported by the solution. In this case, only two blockchain networks are involved and they can have a one-way or request-response interaction following the passive or active mode presented by Jin et al. [26]. On the passive mode, the target blockchain monitors the source blockchain and takes action when an event of interest takes place. The source blockchain does not know the existence of the target chain. The BTC Relay [40] is an example of this mode. On the other hand, on the active model the source chain actively sends information to the target blockchain and waits for a response. Interledger's hashlocking behaviour is an example of active model [41].

4.7 One to many communications

This feature enables interoperability solutions to communicate with many blockchain networks. As the one to one communication feature, it is possible to have communications using the active or passive model, with one-way or request-response interactions. This feature requires a Registry in order to discover the blockchain resources.

4.8 Time lock

The Time lock feature provides time lock capabilities to the blockchain solution. This feature does not allow the execution of a script or transaction until reaching a specified time in the future or a block height [42].

4.9 Hash locks

The Hash lock feature provides hash lock capabilities to the blockchain solution. Hash locking restricts the execution of a script or transaction until some data is publicly provided [43].

4.10 Normalized API

This feature implies that the interoperability solution provides a normalized API to communicate with many blockchain platforms. The Normalized API exposes a set of operations provided by blockchain platforms using a common data format. Source systems (business applications or blockchain platforms) may communicate with other blockchain platforms using this solution as a proxy. The source systems may use a common data format and interface to communicate with the Normalized API. The received message may define the target blockchain of the message and the Normalized API may transform the common data format to the target destination data format. Target blockchain responses may be translated to the common data format of the Normalized API before sending it to the source system. Bifröst, the work presented by Scheid et al. [30], is an example of an interoperability solution with the Normalized API feature.

4.11 Strong business relationship

The strong business relationship feature implies that the blockchains involved have a strong relationship between them and changes in one blockchain have high impact on the other blockchains. In this cases, one blockchain is an extension of another blockchain. The first blockchain cannot exists if the later is not present.

4.12 Observers trigger cross-chain transactions

This feature implies that the interoperability solution requires observers that watch the blockchain and trigger cross-chain transactions to a target blockchain. Observers are an explicit entity on the interoperability solution and can be part of the blockchain or external software system.

4.13 Task coordination

This feature enables interoperability solutions to host business logic coded in some programming language to coordinate tasks between blockchain platforms. For example, the interoperability solution may keep consistency between blockchains on the occurrence of an error by coordinating the transaction registration in two blockchains. If an error occurs, the interoperability solution registers compensation transactions to compensate the execution on the healthy blockchain. The work presented by Xiao et al. [34] is an example of task coordination, where a coordinator exists to keep consistency between the blockchains. The coordinator implements a cross-chain transaction protocol based on three phase commit protocol.

	Public connectors			Blockchain of Blockchains	Enterprise connectors		
Features / Interoperability solution	Notary Scheme	Sidechain/ Relays	Atomic Swaps		Enterprise Relays	Gateway	Generic interface
Connectors	✓	✓		✓	✓	✓	✓
Message adapters	✓	✓		✓	✓	✓	✓
Router				✓	✓		✓
Registry				✓	✓		✓
Relay		✓		✓	✓		
One to one communication	Optional	✓				✓	
One to many communications	✓			✓	✓		✓
Time locks			✓				
Hash locks			✓				
Normalized API					Optional		✓
Strong business relationship		✓		Optional			
Observers trigger cross-chain transactions	✓	✓		✓	Optional	Optional	
Task coordination					Optional		
Requires trust	Optional				Optional	✓	✓

Table 1: Feature-based definition of blockchain interoperability solutions

4.14 Requires trust

This feature defines that the blockchains involved requires some levels of trust in the blockchain interoperability solution. This feature is related to the level of decentralization the interoperability solution provides. The work presented by Bradach et al. [44] requires full trust on the interoperability solution, while the work presented by Liu et al. [45] provides a full decentralized and trustless solution.

5 A Feature-based Definition and Classification of Interoperability Solutions

This work proposes to classify blockchain interoperability solutions into three categories (i.e. Public connectors, Blockchain of blockchains and Enterprise connectors) with six subcategories (i.e. Notary Scheme, Atomic Swaps, Sidechain/ Relays, Enterprise Relays, Gateways and Generic Interface). Table 1 presents the definition of each category based on the feature-based classification framework presented in Section 4. This table clearly specifies when a blockchain interoperability solution belongs to a category, according to the features it supports. The following subsections describe the proposed categories and subcategories. On the other hand, Table 2 presents the application of the classification framework to the reviewed papers. A second level of classification specifies the blockchain interoperability type they apply to. A special column is presented that classifies surveys by its blockchain interoperability type. Finally, this section includes a discussion regarding the proposed feature-based classification framework.

5.1 Public connectors

The Public connectors classification is first introduced by Belchior et al. [11] and is focused on providing blockchain interoperability solutions for cryptocurrency use cases. These solutions mainly involve public blockchain interoperability, but some works used these approaches to provide private to public interoperability [24, 88]. This category can be divided into three subcategories that are described in the next subsections: Notary Scheme, Sidechain/Relays and Atomic Swaps.

5.1.1 Notary Scheme

According to Belchior et al. [11], notary scheme is a trusted third party solution, comprising an entity called notary which monitors multiple blockchains and reacts upon events, by triggering cross-chain transactions

	Public connectors			Blockchain of Blockchains	Enterprise connectors			Review/ Survey
Blockchain Type / Interoperability solution	Notary Scheme	Sidechain/ Relays	Atomic Swaps		Enterprise Relays	Gateway	Generic interface	
Public interoperability	[41, 46, 47]	[22, 48, 49, 50, 51, 52, 53, 54]	[54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69]	[70, 45, 71, 72]		[73, 74]	[75]	[76, 77, 78, 9, 8, 79, 11, 80, 12, 10]
Private interoperability	[81]			[35, 82, 83]	[34, 36, 84, 85]	[73, 86, 44, 74]	[87]	[9, 11, 12, 10]
Public to private interoperability			[88]	[32, 33, 89]		[90, 25, 73, 74, 91]	[30]	[9, 12, 11, 10]

Table 2: Classification of blockchain interoperability academic research using the feature-based classification framework

on another blockchain. Central exchanges (CEXs), such Binance[10] and Coinbase[11], are the most popular type of Notary Scheme and provide users a way to exchange criptocurrencies between different blockchain platforms (e.g. exchange ethers to bitcoins). CEXs own users private keys and executes transactions on behalf of them. In the last years, Decentralized Exchanges (DEXs) started to emerge to offer a decentralized way to exchange criptocurrencies between peers without the need of a centralized party like CEXs. In a DEX, users keep their own private key and exchange their assets between each other using Atomic Swaps or custom Smart contract solutions. Komodo [12] and 0x[13] are two examples of DEXs.

Distributed private key control scheme may be applied to Notary Scheme in order to achieve more security. With this scheme, there are validators which must have a part of the signing key. Each validator generates a signature share with its key and the transaction signature is built by composing each validator's signature share. The transaction is valid only if it has at least the signature share of K validators. This variation follows the Shamir's secret sharing [92] and is used by Wanchain network [93].

5.1.2 Hashed Time Lock Contracts/Atomic swaps

Hash locks consists of an encumbrance that restricts the spending of an output until some data is publicly provided [43]. Time locks, on the other hand, is a type of primitive that restricts the spending of some output until reaching a specified future time or block height [42]. Hash Time Lock Contracts is the combination of this two techniques usually used to implement atomic exchanges of criptocurrencies (also called atomic swaps) between two different blockchains.

Many protocols are available to implement this types of swaps, improving one or another feature [68, 62, 65], but most of them follow the generalized protocol. In this general protocol we have Alice and Bob that want to exchange some assets they have on different blockchain platforms and they follow these steps:

1. Alice has a secret s and generates a hash h of that secret.
2. Alice publishes a smart contract that will only send her asset to Bob if someone presents a secret s. Alice also adds a time lock to her smart contract so that her asset is returned to her after a specified timeout t1 (time lock).
3. Alice gives Bob her hash function and her hash value h and Bob verifies Alice's smart contract is published.

[10] https://www.binance.com
[11] https://www.coinbase.com
[12] https://komodoplatform.com/
[13] https://0x.org/

4. Bob publishes a smart contract that will send his assets to Alice, only after someone presents a secret s, that the hash function of that secret is equal to h (hash lock). Bob's smart contract has also a timelock but with a specified timeout t2. After this timeout expires, his assets will be returned to him. t2 must be less than t1.

5. Alice presents the secret s to Bob's smart contract and Bob learns it. Bob's assets are sent to Alice

6. Bob presents the secret s to Alice's smart contract and Alice's assets are sent to Bob.

In case Alice does not present her secret s to Bob, Bob's assets will be released after timeout t2 expires and Alice's assest will also be released after t1 expires. In case Bob never publishes his smart contract, Alice assets will be released after t1 expires.

5.1.3 Sidechain/relays

Sidechain implies the existence of two blockchains: one that is considered the main chain and keeps the ledger, and a second one, considered the sidechain or secondary chain, that is an extension of the main chain. The communication between them can be one-way (i.e. the main chain sends information to the sidechain), or it can be bi-directional (i.e. both blockchains communicate between each other: two-way peg) [11]. Sidechains communications require a cross-chain (or cross-blockchain) protocol and a relay [11]. The cross-chain (or cross-blockchain) protocol provides the technical layer that enables the correct transfer of messages from the main chain to the sidechain and (optionally) the other way round. On the other hand, Relays are a piece of software hosted on the target chain that verifies the information received from the source chain according to the rules defined in the source chain's consensus protocol. This verification can be made using an SPV [1] or more sophisticated proofs like Zk-SNARKSs [49] or NiPoPoW [94]. Sidechains follow a three layer architecture, where layer 0 is the ledger, layer 1 is the blockchain platform on top of the ledger, and layer 2 is the sidechain. Transactions that occurred on the main chain are called on-chain transactions and follow the main chain consensus protocol, while off-chain transactions are transactions that occurs on the sidechain and follows the sidechain consensus protocol. Most of the times, the sidechain protocol is more efficient than the main chain protocol, to achieve more scalability. Liquid Network [95] is an example of sidechain that adds scalability on top of Bitcoin and RSK [96] is another Bitcoin sidechain that add smart contracts capabilities to it.

5.2 Blockchain of blockchains

As stated by Belchior et al. [11], Blockchain of blockchains is the least studied solution found by this research and its definition is not clear. It is mainly based on industrial examples than academic research. The author describes this interoperability solution as a framework that provides high level features (i.e. consensus, incentives, contract layers) to interoperate application specific blockchains. On the other hand, Siris et al. [8] define it as a *super-ledger*, comprising multiple sidechains connected with a unique main chain. The most advanced work that studied this type of solution is the one presented by Belchior et al. [11] and is the baseline definition of this work.

A Blockchain of blockchains solution is "a system in which a consensus protocol organizes blocks that contain a set of transactions belonging to cross-chain decentralized applications, spread across multiple blockchains. Such a system should provide accountability for the parties issuing transactions on the various blockchains and providing a holistic, updated view of each underlying blockchain" [11].

A Blockchain of blockchains solution has the following building blocks: 1) relays to receive transactions from the source blokchain; 2) a consensus protocol to validate incoming transactions and provide trust to the whole network; 3) connectors and routers to route and send the transaction to the target blockchain; 4) validators on the target blockchain that can validate incoming transactions following the consensus protocol verifications. Cosmos [19] and Polkadot [97] are two industrial examples, while XChange [82] and Hyperservice [45] are two academic examples.

5.3 Enterprise connectors

This work defines the Enterprise connectors as the evolution of the Hybrid connectors category presented by Belchior et al. [11]. The reason for this evolution is that this category is most applied to enterprise environments with certain degree of trust, with the exception of some generic works that are applied to public interoperability (see Table 2). This work also defines new subcategories for the Enterprise Connectors: Gateways, Generic interface and Enterprise relays. These new subcategories are more focused on enterprise requirements and exchange of information than cryptocurrency exchanges, transfer or other Decentralized Finance (DeFi) requirements provided by public connectors solutions.

5.3.1 Gateways

A Gateway middleware is a software that translates two or more protocols. It is in the middle between two software systems intercepting their messages. The Gateway transforms the original message sent by the source system to the format understandable by the recipient software system [98]. Gateways are the most basic interoperability solution that can evolve into a Generic interface or Enterprise relays by adding more features. Gateways provide one to one communication, connectors and message transformer to provide interoperability between software systems (blockchains and applications). Optionally, they can monitor an listen events in the blockchain to trigger cross-chain transactions to a target blockchain. Software systems (Blockchains and application) trust Gateways not to tamper messages nor provide erroneous information to them. Bradach et al. [44] work is an example of a Gateway applied to private interoperability.

5.3.2 Generic interface

The Generic interface subcategory is a type of super service [98] that allows a source system (business application or blockchain platform) to communicate with other blockchain networks using the Normalized API feature. The source system communicates with the Generic interface by sending a common data format message to a common interface it provides. The Generic interface applies data format transformations and use connectors to send the original message to the target blockchain network using its native data format and communication protocols. In case the interaction is a request-response interaction, the Generic interface applies data format transformations and redirect the transformed message to the source system using its native communication protocol. Generic interface solutions requires the Registry feature to discover blockchain platforms and the Routing, Transformation and Connectors features to send messages to the target blockchain platform. Two examples of this type of subcategories are the works presented by Scheid et al. [30] [87].

5.3.3 Enterprise relays

Enterprise relays are the evolution of the Trusted relays categorization defined by Belchior et al. [11] and were first presented in [84]. The present work redefines this subcategory in order to include decentralized capabilities as presented by Ghaemi et al. [36], in order to cope with less trusted environments. The authors of this work consider Enterprise relays provides a better semantic name to this interoperability solution and avoid misunderstandings when using Trusted Relays on an untrusted environment.

Enterprise relays enables blockchain interoperability by receiving cross-chain transaction from a source blockchain and redirecting them to a target blockchain. Enterprise relays have gateway capabilities that allow them to transform message data format and communications protocols between both blockchains. They may also have Registry feature and Routing capabilities to discover blockchain platforms and route messages to them. Finally, they may have Relay capabilities that allow them to validate cross-chain transactions following the source blockchain consensus protocol.

Enterprise relays can be centralized [84] or descentralized [36] and can be configured and deployed on existing blockchain platforms without changing their source code.

5.4 Discussion

Our work proposed a feature-based classification framework that clearly specifies how an interoperability solution is classified without ambiguity. A total of fourteen key features were identified through the analysis of sixty-two blockchain interoperability related papers. These key features were the base for the design of the feature-based classification framework that enabled the classification of the sixty-two surveyed papers according to the features they provide. We think this approach provides a clear classification of blockchain interoperability solutions, giving traceability to the categorization decisions. This supposes a benefit over previous classifications that did not provide details on how they classified the existing work. We think that providing a feature-based definition may help the conceptualization of blockchain interoperability solutions.

Despite these comments, our work presents some limitations. The survey considered academic papers that were published between January 2018 and May 2021, leaving out of scope more updated work that could provide better understanding and conceptualization of blockchain interoperability solutions. Furthermore, the research was performed through full-text assessment only, with no contact with the corresponding authors. This could lead to misunderstanding of the proposed approaches, leading to incorrect identification of features and category classification. In addition, the proposed classification framework involves features with different levels of abstraction that may rise questions about its relevance or suitability. For example, Hash and time locks are more fine grained and lower level features than the Router or Registry feature. This reflects the complexity of the characterization due to the different granularity levels of the features

involved. However, removing hash and time lock features will lead to remove Atomic Swaps, a very relevant interoperability solution in the literature. Finally, we found that the Gateway subcategory is quite similar to the Notary Scheme subcategory when applied to public interoperability. The main difference is quite subtle and refers to the communication mode (i.e. Gateway is a one to one communication while Notary Scheme is a one to many communication). Further analysis is needed to confirm they are conceptually different.

Finally, a better classification can be inspired in other areas of work like middleware, in which there is a clear classification of middleware products. Altman et al. [98] presented a classification based on features where basic middleware provides the foundations for more sophisticated middleware products named platform middleware. Besides our work, further analysis can be performed in this area following a similar approach.

6 Blockchain Interoperability Analysis, Challenges and Research Directions

This section presents a discussion on the landscape of blockchain interoperability state of the art, identifies some challenges as well as open issues, and proposes future research directions.

6.1 Blockchain Interoperability Analysis

As presented in previous sections, there is a large amount of existing work regarding blockchain interoperability, where most of the works focus on public interoperability, tackling challenges related to token transfer and exchange. The majority of the identified works provide new protocols and solutions or improve existing ones. Citizens, DeFi (Decentralized Finance) service providers and blockchain platform providers (e.g. Ethereum) are the main stakeholders of this interoperability type but, as stated by Belchior et al. [11], token exchange is no longer the whole scope of blockchain interoperability. Enterprise organizations started to use the technology and need support for new requirements regarding identity, authorization, consensus protocols, privacy, performance and governance. These requirements are different from public interoperability requirements and need different solutions. Related to this, private and public-to-private interoperability are still on their first steps as little work was found. Some works on private interoperability were performed, but they tackle specific use case requirements and are not a general solution [34, 84]. The status of private-to-public interoperability is not different. Koens et al. [9] presented the first survey that mentions private-to-public interoperability challenges. The authors state that scope, scalability, consensus protocols, cost change state, native token, governance and regulation are some of the challenges in this type of interoperability, but do not provide further details. Later on, Belchior et al. [11] stated that although some critical requirements on blockchain interoperability were fulfilled primary on public blockchain solutions, private and private-to-public interoperability is still a challenge that needs further work. A more recent paper by Lohachab et al. [12] states that there is a need to develop new interoperability solutions that include private and consortium blockchain networks.

In order to start developing interoperability solutions, we first needed to understand the existing ones, their definitions and features. Some interoperability frameworks and classifications exist and have classified them with quite success [9, 11, 12]. Unfortunately, interoperability solutions evolve very fast and classifications become quickly outdated. For example, papers dated on 2019 self classify their work as Sidechains/Relays involving multiple blockchains [32, 33], but nowadays it is more suitable to follow Belchior et al. [11] classification and classify them as Blockchain of blockchains. Another example is that these earlier works only included public interoperability solutions (e.g. Notary Scheme, Sidechains/Relays) and were focused only on cryptocurrency use case scenarios (cryptocurrency exchange and transfer). As stated by Belchior et al. [11], these scenarios are not the whole scope of blockchain interoperability. New types of uses cases (e.g. data exchange) and new types of solutions emerged (e.g. Trusted Relays, Blockchain of blockchains) turning these first works to be incomplete with nowadays state-of-the-art. On the other hand, more recent works dated on 2021 are more updated and include these new types of solutions and provide a more updated survey, but they also have some limitations. They classify the same blockchain interoperability solutions with different categories. For example, Belchior et al. [11] classify Cosmos and Polkadot as a Blockchain of blockchains, but Lohachab et al. [12] classify them as a Relay. How they arrived to these results is not clear as they do not provide details about this decision. A more refined classification is needed to clearly understand blockchain interoperability solutions. In that sense, the present work proposed a feature-based classification framework to aid in this issue, by classifying sixty-two academic papers and identifying three categories (Public connectors, Enterprise connectors and Blockchain of blockchains) with its subcategories (Notary Scheme, Atomic Swaps, Sidechain/Relays, Gateway, Generic interface and Enterprise Relays).

Fig. 7 presents a graphical representation of the relationship between blockchain interoperability solutions and stakeholders. Citizens is a type of stakeholder that includes individual human users. DeFi Service providers are organizations that provide DeFi services to other stakeholders. DeFi services are financial

services that do not rely on a centralized authority to work and use blockchain technology to achieve this goal. Some example of DeFi service providers are Binance[14], Kraken[15] and Coinbase[16] and some examples of DeFi services they provide includes criptocurrency trading, NFT trading, crypto loans, join a liquidity pool and DeFi staking among others. On the other hand, blockchain providers are organizations that provide blockchain platforms to citizens, DeFi Service Providers and enterprise organizations. Some examples are Ethereum, Cardano Foundation, Polygon, Interchain Foundation and Web3 Foundation. These organizations provide among other things, the following blockchain platforms and blockchain interoperability solutions: Ethereum, Cardano, Polygon PoS Bridge, Cosmos and Polkadot. Finally, enterprise organizations are organizations that use private blockchains or a consortium blockchain for the development of their business processes. Some examples are Wallmart or the Italian banks described in Section 2.1.

Public connectors provide interoperability between blockchain platforms or between business applications and blockchain platforms. Citizens may use Notary Scheme and Atomic Swap solutions for some DeFi services between citizens, like critpocurrency exchange and transfer. DeFi Service providers also use these interoperability solutions to offer DeFi services to citizens or organizations. Gateways and Generic Interface solutions may be used to enable connectivity with one or more blockchains. Blockchain providers use Sidechain/Relays to enable token exchange and transfer between public blockchain platforms or improve scalability. Optimism[99], Polygon PoS Bridge[100] and RSK are some examples of Sidechains/Relay. Optimism and Polygon PoS Bridge provide a Sidechain to move assets from Ethereum to Polygon and vice versa, while RSK is a Bitcoin sidechain that allows to execute smart contracts secured by Bitcoin. Public connectors have been studied in the last years and have a large body of literature as it is shown in table 2.

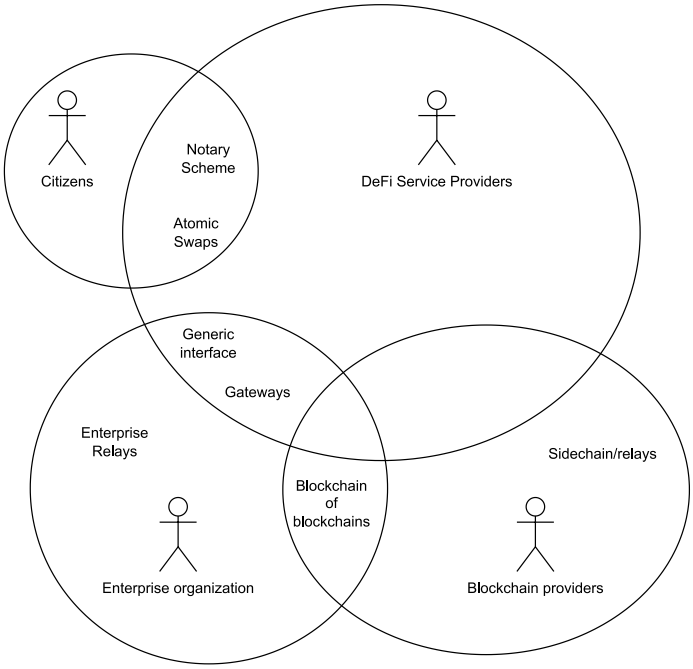

Figure 7: Stakeholders and interoperability solutions.

On the other hand, Enterprise connectors is a new category of blockchain interoperability solutions proposed by our work, more suitable for enterprise interoperability requirements. The citizen is no longer the main user of this type of solutions and business applications take their place. In this case, business applications need to integrate with different blockchain platforms or heterogeneous blockchain platforms need to integrate between each other to fulfill some business process. Token exchange/transfer is no longer the main requirement, which is superseded by data exchange between organizations. Enterprise connectors include Gateways that are trusted software that enables basic interoperability by connecting two blockchain platforms and solving message and protocol differences. Generic interfaces provide a more sophisticated solution and provide a unified Normalized API to integrate a source system (blockchain or application) with many blockchain platforms. Generic interface solutions are still a trusted software and its main role is to simplify interoperability among heterogeneous blockchains. They can be used by other blockchain platforms or by business applications that need to integrate with different blockchain networks. Hyperledger Cactus

[14]https://www.binance.com/
[15]https://www.kraken.com/
[16]https://www.coinbase.com/

or Bifröst are two examples of Generic Interface solution. Enterprise Relays are the most sophisticated piece of software including the previous features of Gateways and Generic interfaces, adding routing, registry and message verification according to the consensus protocols of the involved blockchain platforms. Some Enterprise Relays enable the hosting of business logic rules giving support for coordinated tasks between blockchains. Enterprise relays can be centralized or decentralized. As stated by Belchior et al. [11], Trusted Relays (now renamed Enterprise relays) seems a good solution to private interoperability but further work needs to be done to confirm this hypothesis. There is little work in the area as the solutions are provided for specific use case requirements [84]. A more in-depth study of Enterprise Relays is the work presented by Hardono [74], where he presents a reference architecture, atomicity and security design properties of an Enterprise Relay solution. He also presented challenges regarding identity, crash recovery and discovery, but lacks experimentation. However, as stated by Tam et al. [27], further study is needed to provide a formal analysis, improve blockchain discovery and data consistency. An example of Enterprise Relay is Weaver that enabled interoperability between Corda and Hyperledger Fabric and was used by the Banque de France (the french central bank) to achieve interbank settlement transactions [101].

Blockchain of blockchains is the third category described in this work, for which little research effort was found and further study is needed. To the best of our knowledge, no formal analysis and little experimentation has been performed in this category on academic research.

Finally, as stated by Belchior et al. [11] and confirmed in our research, there are many theoretical works that presents different interoperability solutions, but there is a lack of practical experimentation. Further work is needed here in order to provide and share academic reusable software.

6.2 Challenges and open issues

As presented in other recent surveys, blockchain interoperability is still a challenge [10, 11, 12, 79] and there are several issues that need to be solved in order to have a full trustless descentralized execution of cross-chain transactions [45]. The following subsections present some of these challenges.

6.2.1 Heterogeneous technical aspects

Blockchain interoperability can involve homogeneous (e.g. Ethereum and Polygon) or heterogeneos blockchain platforms (e.g. Ethereum and Bitcoin). Homogeneous blockchain platforms use the same technical primitives (i.e. block size, hash and signature algorithm) and consensus protocol verification that eases interoperability between them. Unless blockchain plataforms are aligned by design (e.g. Bitcoin and Ethereum use the same curve secp256k1 for digital signatures [79]), interoperability solutions need to bridge the technical differences to enable blockchain interoperability. Interoperability solutions needs to bridge heterogeneous models to enable blockchain interoperability.

6.2.2 Heterogeneous models

As presented in Section 2, blockchain networks can be public, private or consortium, having different models regarding user identity, consensus protocols, authorization, privacy and governance. Users on public blockchain use pseudonyms while private blockchain users are clearly identified. Public blockchains use probabilistic consensus protocols that need to be aligned with deterministic protocols used on private blockchains. Privacy is another property that is managed differently on both blockchain types. Besides specific networks like Monero or ZCash, public blockchains traditionally allow other users to see all the transactions written to the ledger, while private blockchains need this information to be kept confidential and only seen by authorized users.

6.2.3 Consistency

The ledger information is immutable, durable and decentralized. Therefore, once information is validated by the consensus protocol, strategies such as two-phase commit and rollback transactions cannot be applied. Eventual consistency is not an option as participants may use the information/asset before a compensation undo the transactions. Related to this, some existing works propose a three-phase commit [34, 35] focused on private interoperability while others focus on escrows and locks [74]. These works seemed to be the first steps in solving consistency issues, but further work is needed. As stated by Tam et al. [27], data consistency on cross-chain transactions cross-spanning multiple blockchain domains is another challenge on blockchain interoperability.

6.2.4 Data protection

Immutability is a key feature on blockchain networks but turns data confidentiality and privacy a hard task to be accomplished. In order to guarantee privacy, data encryption may be suitable in the short term, but encryption algorithms may be obsolete in the future and immutability does not allow to change encrypted data with more powerful algorithms. Data published on public blockchains is immutable and durable forever and nothing assures that nowadays encryption techniques will not be broken in the future. New strategies must be developed in order to cope with these issues. On the other hand, compliance with regulations like the GDPR [102] is not feasible with nowadays definition of immutability on blockchain networks [27]. The "right-to-forget" or the need to delete/update certain data from the blockchain without breaking the chain, is a challenge nowadays.

6.2.5 Blockchain discovery

After our research, we found little work related to blockchain and smart contract discovery [103, 35]. As stated by Tam et al. [27], blockchain discovery may go through the following phases: 1) static and predefined manually, 2) automatic configuration and 3) semantic discovery. Nowadays, there are almost 10.000 cryptocurrencies according to Coinmarket[17] and more private initiatives are rising [84, 34], so manual configuration of blockchain discovery is not feasible. As described by Hardono [80] and Quasse et al. [74], building a decentralized discovery service that enable the discovery of decentralized resources is still a challenge in blockchain interoperability.

6.2.6 Formal analysis on interoperability solutions

Extensive work can be found on formal analysis on Public connectors solutions. For example, Găzi et al.[104] provided a formal analysis on Proof-of-Stake Sidechains, while Kiayias et al. [52] do the same with Proof-of-Work sidechains and Herlihy [62] applied game theory to formalize Atomic swaps. Despite all these efforts, no literature could be found for novel solutions like Belchior et al. categories (e.g. Trusted Relays or Blockchain of Blockchains)[11]. In order to provide reliable interoperability solutions for public-to-private and private interoperability, there is a need to create formal specifications and verification on this type of solutions.

6.2.7 Primitives and patterns

In order to design and build reliable interoperability solutions, patterns and primitives need to be discovered. In this paper we present some features that enable the classification of blockchain solutions, some of which can be seen as patterns or building blocks for blockchain interoperability solutions. An analogy to this is how message brokers, web services middleware, message routing and message transformations are the building blocks of the Enterprise Service Bus [105]. We see the definition, formalization, design and development of blockchain interoperability patterns and primitives is still an open issue and challenge.

6.2.8 Distributed Ledger Technologies interoperability

Most of the research surveyed in this work is focused on blockchain interoperability, being blockchain a specific case of Distributed Ledger Technologies (DLT) [14]. Corda[18] and IOTA[19] are two examples of DLT. To the best of our knowledge there is little research focusing on interoperability between DLT and blockchain as well as on DLT platforms between each other. Two examples are the works presented by Bradach et al. [44] and Jiang et al. [33], which focus on interoperability between Corda and Hyperledger Fabric, but further research is required.

6.3 Future Research Directions

After discussing blockchain interoperability state-of-the-art and challenges, we envision some research questions.

6.3.1 Public to private interoperability solutions

We see private to public interoperability as an untouched area of research and developed the following research questions:

[17] https://coinmarketcap.com/
[18] https://www.corda.net/
[19] https://www.iota.org/

- Is it possible for a user to participate in a cross-chain transaction between public and private blokchains and keep the identity properties of each chain regarding participant anonymity and identification?
- Is it possible that private blockchains validate cross-chain transactions generated on a public blockchains efficiently and in a timely manner and vice-versa?
- Is it possible to keep data properties (e.g. privacy) on cross-chain transactions between private and public blockchains and still follow the consensus protocol on each chain?
- Is it possible to guarantee data consistency on cross-chain transactions between public and private blockchains and keep immutability, durability and decentralization properties?

6.3.2 Patterns and building blocks on blockchain interoperability

The identification of patterns and definition of building blocks for blockchain interoperability is another future direction in blockchain interoperability, for which we rise the following questions:

- Is it possible to identify and define blockchain interoperability patterns?
- Is it possible to define reusable building blocks in order to build blockchain interoperability solutions?
- If blockchain patterns can be defined, is it possible to provide formal analysis tools to help in its development?

6.3.3 Formal analysis on novel blockchain interoperability solutions

We provide the following research question regarding formal analysis on novel blockchain interoperability solutions like Enterprise connectors and Blockchain of blockchains:

- Is it possible to define formal models for Enterprise connectors and Blockchain of blockchains as well as provide formal verification to improve its reliability?
- Is it possible to define a formal taxonomy for blockchain interoperability solutions?

6.3.4 DLT to blockchain interoperability

The following research questions are focused on DLT and blockchain interoperability:

- Is it possible to achieve blockchain and DLT interoperability?
- Does blockchain interoperability solutions may apply to another DLT models like Direct Acyclic Graph networks (e.g. IOTA)?
- Can blockchain interoperability formal models be applied to DLT?

7 Related work

Belchior et al. [11] presented an extensive survey on blockchain interoperability, in which they define blockchain interoperability concepts, a framework to classify blockchain interoperability solutions and a classification of the surveyed articles. This work was the baseline of our work, by taking the proposed classification framework a step further. We provide a feature-based classification framework to clearly categorize blockchain interoperability solutions. We also present other challenges related to blockchain interoperability.

Lohachab et al. [12] presented a survey and a classification framework, in which blockchain interoperability solutions are classified. The work presented a layered architecture based on the OSI stack and a taxonomy to classify blockchain interoperability solutions. The taxonomy is a short categorization that considers use case applications (e.g token transfer), initiator role (passive and active), participation (e.g. heterogeneous DLTs) and interaction (decentralized/centralized). Despite this, this work presented a survey on blockchain interoperability projects and consensus protocols. Our work complements this work with a more refined classification on blockchain interoperability solutions and add blockchain interoperability types to the classification. We share some challenges on blockchain interoperability like anonymity, permissioned blockchain research and consensus protocols related to cross-chain transactions confirmation and propose new challenges.

Koens et al. [9] described a set of properties and a framework to classify interoperability solutions based on twelve key properties related to regulations, scalability, syntactic and semantic interoperability, among

others. Interoperability challenges were presented related to notary scheme, hash lock and sidechain/relays. Furthermore, a brief analysis was performed related to permissioned and permissionless interoperability. We complement Koens et al. work by defining new properties (features) to classify interoperability solutions and include other categories not defined in his work (e.g. blockchains of blockchains). We also provided further discussion on private and public-to-private interoperability, not present in this work.

Siris et al. [8] presented a survey on public blockchain interoperability comparing the following categories: atomic cross-chain transactions, transactions across a network, interledger protocols, bridging solutions, sidechains and ledger-of-ledgers. The authors analyzed these solutions considering transfer and exchange of value, scalability, costs per transaction, complexity and interconnection trust mechanisms. They also presented an initial discussion on blockchain interoperability solutions and a classification, sharing some categories with them. The authors only discussed public interoperability solutions, in contrast with this work that also considers private interoperability and public-to-private interoperability solutions. Our work shows that if we consider a feature-based categorization, some categories presented by the authors can be joined together, providing a more clean and clear categorization of blockchain interoperability solutions. For example, Interledger protocols and Bridges can be categorized as Atomic Swaps, removing redundant categories and create a cleaner categorization.

Monika et al. [76] presented a survey and categorization on blockchain interoperability solutions. The authors define four categories: notary scheme, smart contracts (atomic swaps implemented with smart contracts), blockchain routers and bridging solutions. For each category, they presented its limitations. They also stated that blockchain interoperability between permissioned and non-permissioned blockchains is still a challenge that needs further research. Unfortunately, no further discussion was presented besides this statement. Our work complements this work by providing new categories to classify private interoperability and private-to-public interoperability solutions. We also describe further challenges related to private and public to private interoperability.

Khan et al. [10] analyzed the role of smart contracts in blockchain interoperability, by proposing a taxonomy to classify how blockchain interoperability solutions use smart contracts. They classify some existing solutions and describe some challenges on blockchain interoperability: types of assets exchanged, scalability, privacy and security in cross-chain transactions and compatibility and recovery mechanism. Our work complements the proposed taxonomy by considering features of blockchain interoperability solutions to the classification framework. Besides this, we consider and describe other challenges not present in their work.

Finally, Zamyatin et al. [79] presented a formalization of Cross-Chain Communications (CCC). They also described a framework to categorize CCC protocols depending on the level of trust needed on each phase of the CCC protocol: (Pre-)Commit Phase, Verify Phase, Abort Phase. Levels of trust are categorized by Trusted Third Party, Synchrony Assumptions and Hybrid. Besides this, they also identified some challenges related to public connectors, leaving out of scope enterprise connectors or blockchain of blockchains. Our work complements this paper by considering private-to-public and private interoperability solutions. Zamyatin et al. formalization seems an interesting approach to consider in order to formalize enterprise connectors or blockchains of blockchain.

8 Conclusions

Blockchain interoperability is one of the main topics in the blockchain research area and has evolved quickly during the last years. Indeed, many research and industrial teams are providing different interoperability solutions to different challenges.

The first generation of interoperability solutions involved public blockchains and can be categorized in Notary Scheme, Sidechain/Relays and Atomic Swaps. However, the second generation is still not clear enough, as it involves new solutions (e.g. Blockchains of blockchains) or adds new requirements to solve enterprise use cases on the private blockchain field (e.g. identity management). The characterization and classification of blockchain interoperability solutions is not clear enough in the literature. First works became quickly outdated and later works are sometimes contradictory, with no traceability of classification decisions.

This paper proposed to organize existing work related to blockchain interoperability and understand the features as well as definitions of existing blockchain interoperability solutions. Furthermore, it defines a classification framework to clearly state how blockchain interoperability solutions are classified and why.

The main contributions of this paper include a survey on blockchain interoperability solutions identifying sixty-two relevant papers related to blockchain interoperability. Besides this, a feature-based classification framework was proposed and used fourteen key features to clearly classify blockchain interoperability solutions. As a result, all sixty-two papers were classified based on the defined framework. The classification framework provides three main categories: Public connectors, Blockchains of Blockchain and Enterprise con-

nectors. Each category is also sub-categorized by Notary Scheme, Sidechain/Relay, Atomic Swaps, Gateway, Generic interface and Enterprise Relays. For each subcategory a feature-based definition was proposed.

After the classification and study of these articles, we presented a discussion of the actual state of the art in blockchain interoperability and identified open issues and challenges. Finally, we presented some future research directions that can be the baseline for future research work.

Acknowledgment

Guzmán Llambías was supported by Pyxis.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, (accessed Feb. 2023). [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] SerHack and the Monero Community, Mastering Monero: The future of private transactions. LernoLibro LLC, 2020, (accessed Feb. 2023). [Online]. Available: https://masteringmonero.com/

[3] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in 2014 IEEE Symp. Security and Privacy, Berkeley, CA, USA, May 2014, pp. 459–474. [Online]. Available: https://doi.org/10.1109/SP.2014.36

[4] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014, (accessed Feb. 2023). [Online]. Available: https://ethereum.org/en/whitepaper/

[5] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, 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 Proc. 13th EuroSys Conf., Porto, Portugal, April 2018, pp. 1–15. [Online]. Available: https://doi.org/10.1145/3190508.3190538

[6] R. G. Brown, J. Carlyle, I. Grigg, and M. Hearn, "Corda: An introduction," 2016, (accessed Feb. 2023). [Online]. Available: https://docs.r3.com/en/pdf/corda-introductory-whitepaper.pdf

[7] Cardano Team, "Cardano docs," (accessed Feb. 2023). [Online]. Available: https://docs.cardano.org/introduction

[8] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger approaches," IEEE Access, vol. 7, pp. 89 948–89 966, Jul. 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2926880

[9] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," Pervasive and Mobile Computing, vol. 59, p. 101079, Oct. 2019. [Online]. Available: https://doi.org/10.1016/j.pmcj.2019.101079

[10] S. Khan, M. B. Amin, A. T. Azar, and S. Aslam, "Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability," IEEE Access, vol. 9, pp. 116 672–116 691, Aug. 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3106384

[11] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," ACM Comput. Surv., vol. 54, no. 8, pp. 1–41, Oct. 2021. [Online]. Available: https://doi.org/10.1145/3471140

[12] A. Lohachab, S. Garg, B. Kang, M. B. Amin, J. Lee, S. Chen, and X. Xu, "Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains," ACM Comput. Surv., vol. 54, no. 7, pp. 1–39, Jul. 2021. [Online]. Available: https://doi.org/10.1145/3460287

[13] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Group*, "Preferred reporting items for systematic reviews and meta-analyses: the prisma statement," Annals of internal medicine, vol. 151, no. 4, pp. 264–269, Jul. 2009. [Online]. Available: https://doi.org/10.1371/journal.pmed.1000097

[14] X. Xu, I. Weber, and M. Staples, Architecture for blockchain applications. New York, NY, USA: Springer Cham., 2019.

[15] "Iso 22739:2020. blockchain and distributed ledger technologies — vocabulary," (accessed Feb. 2023). [Online]. Available: https://www.iso.org/standard/73771.html

[16] S. Popov, "The tangle," Apr. 2018, (accessed Feb. 2023). [Online]. Available: http://cryptoverze.s3.us-east-2.amazonaws.com/wp-content/uploads/2018/11/10012054/IOTA-MIOTA-Whitepaper.pdf

[17] P. Windley, "How sovrin works," Oct. 2016, (accessed Feb. 2023). [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/How-Sovrin-Works.pdf

[18] G. Llambías, J. Barreiro, P. Villar, M. Toscano, M. Pereira, and L. González, "Towards a requirement-driven identification and selection process for blockchain platforms," in 2019 XLV Latin American Computing Conference (CLEI), Panama, Panama, Apr. 2019, pp. 1–10. [Online]. Available: https://doi.org/10.1109/CLEI47609.2019.235053

[19] J. Kwon and E. Buchman, "Cosmos whitepaper," (accessed Feb. 2023). [Online]. Available: https://v1.cosmos.network/resources/whitepaper

[20] C. Goes, "The interblockchain communication protocol: An overview," Jun. 2020, (accessed Feb. 2023). [Online]. Available: https://arxiv.org/abs/2006.15918

[21] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," Jan. 2016, (accessed Feb. 2023). [Online]. Available: https://1bitcoin.ca/s/lightning-network-paper.pdf

[22] A. Garoffolo, D. Kaidalov, and R. Oliynykov, "Zendoo: a zk-snark verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains," in 2020 IEEE 40th Int. Conf. Dist. Comp. Sys., Singapore, Singapore, Nov. 2020, pp. 1257–1262. [Online]. Available: https://doi.org/10.1109/ICDCS47774.2020.00161

[23] Weaver Team, "Weaver: Dlt interoperability framework," (accessed Feb. 2023). [Online]. Available: https://labs.hyperledger.org/weaver-dlt-interoperability/

[24] H. Watanabe, S. Ohashi, S. Fujimura, A. Nakadaira, K. Hidaka, and J. Kishigami, "Niji: Autonomous payment bridge between bitcoin and consortium blockchain," in 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, Halifax, NS, Canada, Aug. 2018, pp. 1448–1455. [Online]. Available: https://doi.org/10.1109/Cybermatics_2018.2018.00246

[25] S. Franzoni, "Blockchain and smart contracts in the fashion industry," Master's thesis, Politecnico di Torino, TO, Italy, 2020.

[26] H. Jin, X. Dai, and J. Xiao, "Towards a novel architecture for enabling interoperability amongst multiple blockchains," in 2018 IEEE 38th Int. Conf. Dist. Comp. Sys., Vienna, Austria, Jul. 2018, pp. 1203–1211. [Online]. Available: https://doi.org/10.1109/ICDCS.2018.00120

[27] H. Tam Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of blockchains: Techniques and challenges ahead," in 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, Halifax, NS, Canada, Aug. 2018, pp. 1574–1581. [Online]. Available: https://doi.org/10.1109/Cybermatics_2018.2018.00264

[28] R. Mühlberger, S. Bachhofner, E. Castelló Ferrer, C. Di Ciccio, I. Weber, M. Wöhrer, and U. Zdun, "Foundational oracle patterns: Connecting blockchain to the off-chain world," Business Process Management: Blockchain and Robotic Process Automation Forum, p. 35–51, Sep. 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-58779-6_3

[29] H. Montgomery, H. Borne-Pons, J. Hamilton, M. Bowman, P. Somogyvari, S. Fujimoto, T. Takeuchi, T. Kuhrt, and R. Belchior, "Hyperledger cactus whitepaper," Mar. 2022, (accessed Feb. 2023). [Online]. Available: https://github.com/hyperledger/cactus/blob/main/whitepaper/whitepaper.md

[30] E. J. Scheid, T. Hegnauer, B. Rodrigues, and B. Stiller, "Bifröst: a modular blockchain interoperability api," in IEEE 44th Conference Local Computer Networks, Osnabrueck, Germany, Feb. 2019, pp. 332–339. [Online]. Available: https://doi.org/10.1109/LCN44214.2019.8990860

[31] M. He, X. Han, F. Jiang, R. Zhang, X. Liu, and X. Liu, "Blockmeds: A blockchain-based online prescription system with privacy protection," in Service-Oriented Computing – ICSOC 2019 Workshops, Toulouse, France, Oct. 2020, pp. 299–303. [Online]. Available: https://doi.org/10.1007/978-3-030-45989-5_27

[32] Z. Zhang, C. Zhong, S. Guo, and F. Wang, "A master-slave chain architecture model for cross-domain trusted and authentication of power services," in Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City, New York, NY, USA, Dec. 2019, p. 483–487. [Online]. Available: https://doi.org/10.1145/3377170.3377225

[33] Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A cross-chain solution to integrating multiple blockchains for iot data management," Sensors, vol. 19, no. 9, p. 2042, May 2019. [Online]. Available: https://doi.org/10.3390/s19092042

[34] X. Xiao, Z. Yu, K. Xie, S. Guo, A. Xiong, and Y. Yan, "A multi-blockchain architecture supporting cross-blockchain communication," in Artificial Intelligence and Security, Hohhot, China, Jul. 2020, pp. 592–603. [Online]. Available: https://doi.org/10.1007/978-981-15-8086-4_56

[35] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, Jul. 2018, pp. 139–145. [Online]. Available: https://doi.org/10.1109/QRS-C.2018.00037

[36] S. Ghaemi, S. Rouhani, R. Belchior, R. S. Cruz, H. Khazaei, and P. Musilek, "A pub-sub architecture to promote blockchain interoperability," Jan. 2021, (accessed Feb. 2023). [Online]. Available: https://arxiv.org/abs/2101.12331

[37] G. Hohpe and B. Woolf, Enterprise integration patterns: Designing, building, and deploying messaging solutions. Boston, MA, USA: Addison-Wesley Professional, 2004.

[38] C. Richardson, "Pattern: Service registry," (accessed Feb. 2023). [Online]. Available: https://microservices.io/patterns/service-registry.html

[39] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," Expert Systems with Applications, vol. 168, p. 114384, Apr. 2021. [Online]. Available: https://doi.org/10.1016/j.eswa.2020.114384

[40] BTC Relay Team, "A bridge between the bitcoin blockchain & ethereum smart contracts," (accessed Feb. 2023). [Online]. Available: http://btcrelay.org/

[41] S. Thomas and E. Schwartz, "A protocol for interledger payments," 2015, (accessed Feb. 2023). [Online]. Available: https://interledger.org/interledger.pdf

[42] Bitcoin wiki, "Timelock," (accessed Feb. 2022). [Online]. Available: https://en.bitcoin.it/wiki/Timelock

[43] Bitcoin Wiki, "Hashlock," (accessed Feb. 2022). [Online]. Available: https://en.bitcoin.it/wiki/Hashlock

[44] B. Bradach, J. Nogueira, G. Llambías, L. González, and R. Ruggia, "A gateway-based interoperability solution for permissioned blockchains," in 2022 XVLIII Latin American Computer Conference (CLEI), Armenia, Colombia, Oct. 2022, pp. 1–10. [Online]. Available: https://doi.org/10.1109/CLEI56649.2022.9959907

[45] 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, New York, NY, USA, Nov. 2019, p. 549–566. [Online]. Available: https://doi.org/10.1145/3319535.3355503

[46] K. Sai and D. Tipper, "Disincentivizing double spend attacks across interoperable blockchains," in 2019 1st IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), Los Angeles, CA, USA, Dec. 2019, pp. 36–45. [Online]. Available: https://doi.org/10.1109/TPS-ISA48467.2019.00014

[47] D. Li, J. Liu, Z. Tang, Q. Wu, and Z. Guan, "Agentchain: A decentralized cross-chain exchange system," in 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, Aug. 2019, pp. 491–498. [Online]. Available: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00072

[48] 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), Rhodes, Greece, Nov. 2020, pp. 204–213. [Online]. Available: https://doi.org/10.1109/Blockchain50366.2020.00032

[49] 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), Genoa, Italy, Sep. 2020, pp. 378–386. [Online]. Available: https://doi.org/10.1109/EuroSPW51379.2020.00058

[50] S. Daveas, K. Karantias, A. Kiayias, and D. Zindros, "A gas-efficient superlight bitcoin client in solidity," in Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, Oct. 2020, p. 132–144. [Online]. Available: https://doi.org/10.1145/3419614.3423255

[51] A. Zamyatin, Z. Avarikioti, D. Perez, and W. J. Knottenbelt, "Txchain: Efficient cryptocurrency light clients via contingent transaction aggregation," in Data Privacy Management, Cryptocurrencies and Blockchain Technology, Guildford, UK, Sep. 2020, pp. 269–286. [Online]. Available: https://doi.org/10.1007/978-3-030-66172-4_18

[52] A. Kiayias and D. Zindros, "Proof-of-work sidechains," in Financial Cryptography and Data Security, St. Kitts, St. Kitts and Nevis, Feb. 2020, pp. 21–34. [Online]. Available: https://doi.org/10.1007/978-3-030-43725-1_3

[53] M. Westerkamp and M. Diez, "Verilay: A verifiable proof of stake chain relay," in 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China, May 2022, pp. 1–9. [Online]. Available: https://doi.org/10.1109/ICBC54727.2022.9805554

[54] 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), San Francisco, CA, USA, May 2019, pp. 193–210. [Online]. Available: https://doi.org/10.1109/SP.2019.00085

[55] L. Lys, A. Micoulet, and M. Potop-Butucaru, "Atomic swapping bitcoins and ethers," in 2019 38th Symposium on Reliable Distributed Systems (SRDS), Lyon, France, Oct. 2019, pp. 372–3722. [Online]. Available: https://doi.org/10.1109/SRDS47363.2019.00054

[56] M. Darisi, J. Savla, M. Shirole, and S. Bhirud, "Stem: Secure token exchange mechanisms," in Advances in Cyber Security, Penang, Malaysia, Jul. 2020, pp. 206–219. [Online]. Available: https://doi.org/10.1007/978-981-15-2693-0_15

[57] N. Shadab, F. Houshmand, and M. Lesani, "Cross-chain transactions," in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, May 2020, pp. 1–9. [Online]. Available: https://doi.org/10.1109/ICBC48266.2020.9169477

[58] Monika, A. Goyal, S. Raina, K. Bhatia, and R. Bhatia, "Atomic cross-chain asset exchange for ethereum public chains," in 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, Jan. 2021, pp. 1–4. [Online]. Available: https://doi.org/10.1109/ICCCI50826.2021.9402343

[59] M. Tefagh, F. Bagheri, A. Khajehpour, and M. Abdi, "Atomic bonded cross-chain debt," in 3rd International Conference on Blockchain Technology and Applications, Xi'an, China, Dec. 2020, p. 50–54. [Online]. Available: https://doi.org/10.1145/3446983.3446987

[60] L. Cao and Z. Wan, "Anonymous scheme for blockchain atomic swap based on zero-knowledge proof," in 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, Jun. 2020, pp. 371–374. [Online]. Available: https://doi.org/10.1109/ICAICA50127.2020.9181875

[61] V. Zakhary, D. Agrawal, and A. El Abbadi, "Atomic commitment across blockchains," Proc. VLDB Endow., vol. 13, no. 9, p. 1319–1331, May 2020. [Online]. Available: https://doi.org/10.14778/3397230.3397231

[62] M. Herlihy, "Atomic cross-chain swaps," in Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Egham United Kingdom, Jul. 2018, p. 245–254. [Online]. Available: https://doi.org/10.1145/3212734.3212736

[63] S. Yang, H. Wang, W. Li, W. Liu, and X. Fu, "Cvem: A cross-chain value exchange mechanism," in Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things, Singapore, Singapore, Oct. 2018, p. 80–85. [Online]. Available: https://doi.org/10.1145/3291064.3291073

[64] L. Lys, A. Micoulet, and M. Potop-Butucaru, "Atomic cross chain swaps via relays and adapters," in Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, London, United Kingdom, Sep. 2020, p. 59–64. [Online]. Available: https://doi.org/10.1145/3410699.3413799

[65] S. Imoto, Y. Sudo, H. Kakugawa, and T. Masuzawa, "Atomic cross-chain swaps with improved space and local time complexity," in Stabilization, Safety, and Security of Distributed Systems, Pisa, Italy, Oct. 2019, pp. 194–208. [Online]. Available: https://doi.org/10.1007/978-3-030-34992-9_16

[66] J.-Y. Zie, J.-C. Deneuville, J. Briffaut, and B. Nguyen, "Extending atomic cross-chain swaps," in Data Privacy Management, Cryptocurrencies and Blockchain Technology, Luxembourg, Luxembourg, Sep. 2019, pp. 219–229. [Online]. Available: https://doi.org/10.1007/978-3-030-31500-9_14

[67] M. Herlihy, B. Liskov, and L. Shrira, "Cross-chain deals and adversarial commerce," Proc. VLDB Endow., vol. 13, no. 2, p. 100–113, Oct. 2019. [Online]. Available: https://doi.org/10.1007/s00778-021-00686-1

[68] A. Deshpande and M. Herlihy, "Privacy-preserving cross-chain atomic swaps," in Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, Feb. 2020, pp. 540–549. [Online]. Available: https://doi.org/10.1007/978-3-030-54455-3_38

[69] L. Deng, H. Chen, J. Zeng, and L.-J. Zhang, "Research on cross-chain technology based on sidechain and hash-locking," in Edge Computing – EDGE 2018, Seattle, WA, USA, Jun. 2018, pp. 144–151. [Online]. Available: https://doi.org/10.1007/978-3-319-94340-4_12

[70] Z. Xu, J. Zhang, Z. Song, Y. Liu, J. Li, and J. Zhou, "A scheme for intelligent blockchain-based manufacturing industry supply chain management," Computing, vol. 103, pp. 1771–1790, Jan. 2021. [Online]. Available: https://doi.org/10.1007/s00607-020-00880-z

[71] G.-Y. Yang, K.-H. Yeh, and L.-F. Lee, "Towards a novel interoperability management scheme for cross-blockchain transactions," in 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE), Kyoto, Japan, Oct. 2021, pp. 942–943. [Online]. Available: https://doi.org/10.1109/GCCE53005.2021.9621818

[72] G. Sagirlar, J. D. Sheehan, and E. Ragnoli, "On the design of co-operating blockchains for iot," in 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, Mar. 2020, pp. 548–552. [Online]. Available: https://doi.org/10.1109/ICICT50521.2020.00093

[73] T. Hardjono, A. Lipton, and A. Pentland, "Toward an interoperability architecture for blockchain autonomous systems," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1298–1309, Nov. 2020. [Online]. Available: https://doi.org/10.1109/TEM.2019.2920154

[74] T. Hardjono, "Blockchain gateways, bridges and delegated hash-locks," Feb. 2021, (accessed Feb. 2023). [Online]. Available: https://arxiv.org/abs/2102.03933

[75] W. Cai and X. Wu, "Demo abstract: An interoperable avatar framework across multiple games and blockchains," in IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Apr. 2019, pp. 967–968. [Online]. Available: https://doi.org/10.1109/INFCOMW.2019.8845288

[76] Monika and R. Bhatia, "Interoperability solutions for blockchain," in 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, Dec, 2020, pp. 381–385. [Online]. Available: https://doi.org/10.1109/ICSTCEE49637.2020.9277054

[77] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, "Towards blockchain interoperability," in Business Process Management: Blockchain and Central and Eastern Europe Forum, Vienna, Austria, Sep. 2019, pp. 3–10. [Online]. Available: https://doi.org/10.1007/978-3-030-30429-4_1

[78] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Blockchain interoperable digital objects," in Blockchain – ICBC 2019, San Diego, CA, USA, Jun. 2019, pp. 80–94. [Online]. Available: https://doi.org/10.1007/978-3-030-23404-1_6

[79] 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, Virtual Event, Mar. 2021, pp. 3–36. [Online]. Available: https://doi.org/10.1007/978-3-662-64331-0_1

[80] I. A. Qasse, M. Abu Talib, and Q. Nasir, "Inter blockchain communication: A survey," in Proceedings of the ArabWIC 6th Annual International Conference Research Track, Rabat, Morocco, Mar. 2019. [Online]. Available: https://doi.org/10.1145/3333165.3333167

[81] Z. Gao, H. Li, K. Xiao, and Q. Wang, "Cross-chain oracle based data migration mechanism in heterogeneous blockchains," in 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore, Feb. 2020, pp. 1263–1268. [Online]. Available: https://doi.org/10.1109/ICDCS47774.2020.00162

[82] M. de Vos, C. U. Ileri, and J. Pouwelse, "Xchange: A universal mechanism for asset exchange between permissioned blockchains," World Wide Web, vol. 24, no. 5, pp. 1–38, Sep. 2021. [Online]. Available: https://doi.org/10.1007/s11280-021-00870-x

[83] X. Hu, K. Hu, S. Wang, and Q. Tong, "A master-slave chain model for multiple blockchains," in 2020 the 3rd International Conference on Blockchain Technology and Applications, Xi'an, China, Dec. 2020, p. 12–18. [Online]. Available: https://doi.org/10.1145/3446983.3446988

[84] 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, Dec. 2019, p. 29–35. [Online]. Available: https://doi.org/10.1145/3366626.3368129

[85] 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://doi.org/10.1016/j.future.2021.11.004

[86] C. Lin and Z. W. Zhang, "A two-tier blockchain architecture for the digital transformation of multilateralism," in 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, Jun. 2020, pp. 1–5. [Online]. Available: https://doi.org/10.1109/VTC2020-Spring48590.2020.9128957

[87] E. Scheid, B. Rodrigues, and B. Stiller, "Toward a policy-based blockchain agnostic framework," in 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, Apr. 2019, pp. 609–613.

[88] Z. Li and Z. Zhang, "Research and implementation of multi-chain digital wallet based on hash timelock," in Blockchain and Trustworthy Systems, Guangzhou, China, Dec. 2020, pp. 175–182. [Online]. Available: https://doi.org/10.1007/978-981-15-2777-7_15

[89] Q. Yang, H. Guo, V. Zhu, X. Fan, X. Cui, X. Kong, and B. K. Bobby, "A novel sustainable interchain network framework for blockchain," in Smart Blockchain, Tokyo, Japan, Dec. 2018, pp. 111–119. [Online]. Available: https://doi.org/10.1007/978-3-030-05764-0_12

[90] G. Falazi, U. Breitenbücher, F. Daniel, A. Lamparelli, F. Leymann, and V. Yussupov, "Smart contract invocation protocol (scip): A protocol for the uniform integration of heterogeneous blockchain smart contracts," in Advanced Information Systems Engineering, Grenoble, France, Jun. 2020, pp. 134–149. [Online]. Available: https://doi.org/10.1007/978-3-030-49435-3_9

[91] S. Punathumkandi, V. M. Sundaram, and P. Panneer, "Interoperable permissioned-blockchain with sustainable performance," Sustainability, vol. 13, no. 20, p. 11132, Oct. 2021. [Online]. Available: https://doi.org/10.3390/su132011132

[92] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, p. 612–613, Nov. 1979. [Online]. Available: https://doi.org/10.1145/359168.359176

[93] Wanchain Team, "Wanchain," (accessed Feb. 2023). [Online]. Available: https://docs.wanchain.org/get-started/introduction

[94] A. Kiayias, A. Miller, and D. Zindros, "Non-interactive proofs of proof-of-work," in Financial Cryptography and Data Security, Kota Kinabalu, Malaysia, Feb. 2020, pp. 505–522. [Online]. Available: https://doi.org/10.1007/978-3-030-51280-4_27

[95] J. Nick, A. Poelstra, and G. Sanders, "Liquid: A bitcoin sidechain," May 2020, (accessed Feb. 2023). [Online]. Available: https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf

[96] S. D. Lerner, J. Álvarez Cid-Fuentes, J. Len, R. Fernàndez-València, P. Gallardo, N. Vescovo, R. Laprida, S. Mishra, F. Jinich, and D. Masini, "Rsk: A bitcoin sidechain with stateful smart-contracts," May 2022, (accessed Feb. 2023). [Online]. Available: https://eprint.iacr.org/2022/684

[97] Web3 Foundation, "An introduction to polkadot," Apr. 2020, (accessed Feb. 2023). [Online]. Available: https://polkadot.network/Polkadot-lightpaper.pdf

[98] R. Altman, Y. Natis, J. Hill, J. Klein, B. Lheureux, M. Pezzini, R. Schulte, and S. Varma, "Middleware: The glue for modern applications," Jul 1999, (accessed Feb. 2023). [Online]. Available: https://www.gartner.com/en/documents/300144

[99] Optimism Team, "Bridging basics," (accessed Feb. 2023). [Online]. Available: https://community.optimism.io/docs/developers/bridge/basics/

[100] Polygon Team, "Introduction to polygon pos," (accessed Feb. 2023). [Online]. Available: https://wiki.polygon.technology/docs/develop/getting-started

[101] Ledger Insights, "Banque de france completes final wholesale cbdc trial with hsbc," Dic. 2021, (accessed Feb. 2023). [Online]. Available: https://www.ledgerinsights.com/banque-de-france-wholesale-cbdc-trial-with-hsbc/

[102] F. Molina, G. Betarte, and C. Luna, "Design principles for constructing gdpr-compliant blockchain solutions," in 2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), Madrid, Spain, May 2021, pp. 1–8. [Online]. Available: https://doi.org/10.1109/WETSEB52558.2021.00008

[103] A. Lamparelli, G. Falazi, U. Breitenbücher, F. Daniel, and F. Leymann, "Smart contract locator (scl) and smart contract description language (scdl)," in 2019 International Conference on Service-Oriented Computing, Toulouse, France, Oct. 2019, p. 195–210. [Online]. Available: https://doi.org/10.1007/978-3-030-45989-5_16

[104] P. Gaži, A. Kiayias, and D. Zindros, "Proof-of-stake sidechains," in 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, Sep. 2019, pp. 139–156. [Online]. Available: https://doi.org/10.1109/SP.2019.00040

[105] D. Chappell, Enterprise Service Bus. O'Reilly Media, Inc., 2004.

[106] A. Culwick and D. Metcalf, "Blocknet design specifications," Mar. 2018, (accessed Feb. 2023). [Online]. Available: https://docs.blocknet.org/project/blocknet-whitepaper.pdf

[107] ARK Team, "Ark ecosystem whitepaper," Sep. 2019, (accessed Feb. 2023). [Online]. Available: https://ark.io/Whitepaper.pdf

[108] Datachain, "Yui," (accessed Feb. 2023). [Online]. Available: https://www.datachain.jp/products/yui

Appendix 1: Industrial Interoperability Solutions

This section describes some of the industrial interoperability approaches and groups them according to its interoperability type (public, private or private to public interoperability).

Public interoperability solutions

Polygon network [100] (previously known as Matic Network) is a public blockchain that enables interoperability with the Ethereum blockchain by using two interoperability solutions: Plasma and PoS bridges. With Plasma and PoS bridges, Polygon behaves as a two-way peg sidechain of the Ethereum blockchain, where assets can be moved from Ethereum to Polygon and the other way round. The PoS bridge is composed of a set of smart contracts that help to move assets between Ethereum and Polygon. There exists a Root Manager Token contract on Ethereum blockchain and a Child Manager Token contract on Polygon blockchain. When an asset is locked on the Root Manager Token contract, an event is triggered to the Child Manager Token contract to create an asset semantically equivalent on Polygon. When this new token is no longer needed, the token can be returned to Ethereum by burning it on Polygon. When the new token is burned, an event is triggered on the Root Manager Token contract with a proof that the token was burned. The Root Manager Token contract will validate the proof and unlock the previously locked token on Ethereum. Plasma bridge works in a similar way but provides increased security after burning the new token on Polygon. Plasma defines a 7-day withdrawal period. When the user burns the tokens on Polygon, an Exit NFT token is created on Ethereum with the semantic equivalent value. After the 7-day withdrawal period expires, the user can claim back the locked tokens on Ethereum by using the process-exit procedure. Other users can present fraud proofs in this 7-day period in case they find that the withdrawal is not allowed. The later provides more security to the Plasma bridge than the PoS bridge.

Ethereum Optimism [99] is another public blockchain that provides interoperability with Ethereum using a Sidechain solution similar to Polygon Plasma bridge. Ethereum Optimism provides smart contracts that acts as bridges to move assets from Ethereum to Optimism and vice versa. To move asset to Ethereum, the user needs to call the bridge smart contracts on Ethereum that will lock this asset for future usage. This smart contract will make a direct communication with the bridge smart contracts on Optimism and a new semantic equivalent asset on Optimism is created. To return the asset from Optimism to Ethereum, the user needs to call the bridge smart contract on Optimism to make the withdrawal. After that, the asset at Optimism is burned but the user cannot claim on Ethereum yet. The user needs to wait a 7-day period that enables other users to submit fraud proofs to Ethereum in case it is a fraud transaction.

Blocknet is a Proof-of-Stake blockchain that provides peer-to-peer interoperability between nodes on different blockchains [106]. Blocknet protocol is composed by two components called XBridge and XRouter. XBridge provides the infrastructure to enable the exchange of tokens on a decentralized and trustless manner by using BIP65 CLTV[20] atomic swaps contracts or similar methods for other blockchains that do not provide this technical construct. On the other hand, XRouter provides the blockchain interoperability infrastructure to the Blocknet protocol by providing blockchain lookup, registry services and SPV clients for cross-chain transactions validations. By design, Blocknet may support private and public blockchains but nowadays Blocknet supports only public blockchains [21].

ARK mainnet is a public blockchain that follows the Delegated Proof-of-Stake (DPoS) and supports blockchain interoperability through its SmartBridge Technology which provides two protocols: 1) Protocol-Specific SmartBridge and 2) Protocol-Agnostic SmartBridge [107]. The first protocol provides homogeneous interoperability between ARKs networks by using events and listeners on a bridge ARK chain. The bridge ARK chain acts as a proxy providing a decentralized solution that routes cross-chain transactions from a source ARK network to a target ARK network. The second protocol is an open source project called ARK Contract Execution Services (ACES) that enables heterogeneous interoperability between ARK and other blockchain platforms. It follows a similar approach of events and listeners and requires blockchain platforms to add pieces of code to support vendor fields to tag their transactions. External tagged transactions are monitored by Encoded Event Listener nodes that route transactions to the target blockchain (e.g. ARK, other blockchain). A more recent solution for blockchain interoperability is based on HTLC but it is still in experimental phase[22]. Some proofs-of-concepts have been carried out to achieve interoperability between ARK and Hyperledger Fabric[23]. ARK supports Bitcoin, Ethereum and Litecoin[24].

[20] https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki
[21] https://docs.blocknet.co/protocol/xbridge/compatibility/
[22] https://github.com/ArkEcosystem/AIPs/blob/master/AIPS/aip-102.md
[23] https://ark.io/blog/making-cross-chain-smart-contracts-on-ark-via-hyperledger-fabric-e69149b1e12c
[24] https://datascience.foundation/sciencewhitepaper/ark-stack-development-an-interoperability-solution-for-seamless-blockchain-ecosystem

Private interoperability solutions

Hyperledger Cactus is a framework that provides an abstraction on top of blockchain networks to enable enterprise applications to interoperate with them [29]. It provides an extensible plugin architecture that enables the integration of new blockchain networks supporting the following blockchain platforms: Hyperledger Fabric, Hyperledger Besu, Corda and Quorum. It provides interoperability validators hosted on the source and target blockchains that receive, sign and verify the messages exchanged between them. Hyperledger cactus is an application-to-blockchain interoperability solution.

Weaver is another framework similar to Hyperledger Cactus that enables interoperability between enterprise applications and blockchain networks [84]. Each network must have an IOP Module plus a Trusted Relay [11]. Relays enable applications to connect with a source blockchain network to query data and the IOP module allows them to store this data, following the target blockchain network verification policies (i.e. consensus protocol). The IOP module also has the responsibility to apply the verification policies of external requests made by a source blockchain network Relay. Nowadays, Weaver supports Hyperledger Fabric, Hyperledger Besu and Corda. Weaver is an application-to-blockchain interoperability solution.

YIU is a Hyperledger Labs project that enables interoperability between heterogeneous blockchain networks [108] by implementing the IBC protocol [20]. Each blockchain network has an IBC Module that allows to communicate with other blockchains through a Relayer. The IBC Module verifies received messages following the target network verification policies. For example, the IBC Module of Hyperledger Besu may verify the message header for IBFT 2.0, while the IBC Module of Hyperledger Fabric may verify the endorsements' signatures. The main difference between YIU and Hyperledger Cactus or Weaver is that YUI provides a platform-to-platform interoperability instead of application-to-platform interoperability provided by those solutions. Nowadays, YUI supports Hyperledger Besu, Hyperledger Fabric and Corda.

Public to private interoperability solutions

Cosmos is a network of independent blockchains that follow a Proof-of-Stake protocol called Tendermint to achieve consensus [19]. Each blockchain is called a Cosmo Zone and the first connected blockchain is called Cosmo Hub. The Hub connects to other zones using the IBC protocol [20] and tracks the different token types and records the number of tokens existing in each zone. Transfer of assets between zones is done in a secure manner without the need of liquidity exchange between zones as all the transfer exchange is done through the Cosmos Hub. Nowadays, there are IBC Modules for Hyperledger Fabric[25], Corda[26] and Ethereum[27], which enable interoperability between these blockchain networks.

Polkadot is a project similar to Cosmos and is composed of a network of heterogeneous blockchain networks called parachain [97]. Parachains are connected between each other by the Polkadot Relay Chain, an entity that is responsible for the network's security, consensus and blockchain interoperability. Parachains are independent blockchain networks that have their own tokens and functionality for specific use cases. Bridges are another type of entity in Polkadot that enable external blockchain networks (i.e. Bitcoin, Ethereum) to be connected to Polkadot, and enable the communication with parachains. Chain Bridge is an effort to provide a bridge to connect Ethereum with Moonbean, a Polkadot parachain. At the time of writing this work, no bridges were found for private blockchains like Hyperledger Fabric or Corda, although is theoretically supported.

[25] https://github.com/hyperledger-labs/yui-fabric-ibc
[26] https://github.com/hyperledger-labs/yui-corda-ibc
[27] https://github.com/cosmos/gravity-bridge