Characterizing Blockchain Interoperability Systems from an Architecture Perspective

João Otávio Chervinski[1,2(✉)], Jiangshan Yu[1], and Xiwei Xu[2,3]

[1] Monash University, Melbourne, Australia
joao.massarichervinski@monash.edu
[2] CSIRO Data61, Eveleigh, Australia
[3] University of New South Wales, Sydney, Australia

Abstract. Blockchains are designed as closed execution environments that only support operations within their own system for security purposes. However, as the technology became popular, interoperation across different blockchains emerged as one of the most desired features to enable the creation of networks of interconnected blockchains. Towards fulfilling this need, multiple academic proposals and industry projects have been developed, but most of those systems are designed to connect specific platforms and cannot be applied to all blockchains. While there are studies that aim to provide understanding on these solutions, they are mainly focused on the cryptographic formalization and dependability of such systems. Limited attention has been paid to the system architecture and organization of such solutions. This paper aims to bridge this gap by characterizing existing cross-chain communication systems from an architecture perspective. We classify ten existing systems into four categories and develop an evaluation framework with criteria from five different aspects. We then evaluate the selected systems based on the proposed framework and present a comparative analysis between the systems in each category. We aim to provide an holistic view of state-of-practice to help developers and the blockchain community to select suitable solutions for their cross-chain communication needs.

Keywords: Distributed ledgers · Blockchains · Interoperability · Cross-chain communication

1 Introduction

Over the last decade blockchain technologies and their applications underwent rapid growth [10,21,28,32,39] leading the number of existing blockchains to surge. This contributed to an increase in blockchain diversity and led to the creation of a host of chains with distinct objectives such as providing transaction privacy [29,30], bridging fiat money and cryptocurrencies [33] or providing smart contract functionality [7].

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 504–520, 2022.
https://doi.org/10.1007/978-3-031-06371-8_33

However, when users want to make use of diverse functionalities they must purchase coins in distinct blockchains or exchange their assets for other cryptocurrencies. One popular solution for exchanging assets is using exchange services. This approach, however, has high trading fees, low transparency and reduced security as those services are often targeted by criminals [34].

Blockchain interoperability systems aim to fill this gap by enabling communication between blockchains. Interoperability has been deemed critical for the advancement of the blockchain technology [4] thus the interest in this area of research is growing. Multiple academic proposals [3,13,15,18,20,38] and industry projects [11,16,22,27,31,35] have been proposed to address this challenge.

However, differences in security mechanisms, protocols and scripting capabilities can all pose challenges for cross-chain communication systems. For that reason, many interoperability solutions are developed for specific pairs of blockchains [6].

While existing research provides comprehensive review on the existing systems [4,6,37], a holistic view from the architecture perspective remains unclear. Such a big picture is important to aid developers in the process of understanding the different characteristics of the existing solutions and selecting the ones which meet their needs. In this paper, we bridge this gap by characterizing blockchain interoperability solutions from an architecture perspective.

The main contributions of this paper are summarized as follows: (a) we classify ten leading blockchain interoperability systems into four categories based on their characteristics; (b) we propose an evaluation framework with criteria from five different architectural aspects; (c) we evaluate ten cross-chain communication systems based on the proposed framework; (d) we compare the cross-chain communication systems in each category by analyzing their strengths and weaknesses.

Our framework provides design guidance to assist developers in selecting interoperability solutions that are suitable to their use-cases. Our analysis provides support in the assessment of the benefits and drawbacks of interoperability system categories and individual systems given developer's specific requirements. Throughout this work we refer to blockchain interoperability and cross-chain communication interchangeably.

This paper is organised as follows. Section 2 characterizes the architectures of cross-chain communication systems. Section 3 presents our proposed evaluation framework and Sect. 4 presents a detailed analysis of the system categories and the ten leading systems. Finally, Sect. 5 presents related work and Sect. 6 presents concluding remarks.

2 Interoperability Categories

In this section we propose four categories to characterize and distinguish blockchain interoperability systems. We define blockchain interoperability as the ability to provably transfer information between two distinct blockchains in a semantically compatible format.

The proposed categories were derived from the analysis and comparison of both the architecture and functionality provided by ten leading cross-chain communication systems. The systems we selected are either from academia [11,13,15,18,20] and known by the research community or well-known industrial projects [8,16,22,27,35]. We have selected those systems as we believe they provide a reasonable overview of the state-of-the-art of cross-chain communications. A detailed analysis of each category and its corresponding systems is provided in Sect. 4. Through our analysis of the selected systems we identified four distinct categories of cross-chain communication systems:

Blockchain ecosystems manage networks of independent blockchains that are interconnected through a central chain or hub that forwards information. Ecosystems enable native cross-chain communication between blockchains inside the network and can also allow communication with external blockchains through bridging systems. Blockchain ecosystems have their own native tokens which can be used for stake-based consensus and for voting in feature proposals. Those systems can be permissioned or permissionless. *Cosmos* [22] and *Polkadot* [5] belong to this category.

Relay-Based systems enable a blockchain (called the destination chain) to fetch and validate data coming from a source blockchain. The destination blockchain needs to implement the consensus verification mechanism of the source chain in order to verify the validity of the information received through the relay. A single relay system allows the destination chain to verify events that took place in a source chain, however the contrary is not necessarily true and may require two relays, one in each chain. This category of system includes *BTC Relay* [8], *ETH Relay* [11] and *Proof-of-Burn (PoB)* [20].

Sidechain-based systems are constructions that connect two blockchains and allow them to transfer assets back and forth between each other via a process called a two-way peg [3]. Sidechain-based systems aim to enable users of a blockchain to transfer their assets to another blockchain, called a sidechain, and use those assets to access features and applications not available in the source blockchain. The systems included in this category are *Liquid Network* [27], *Proof-of-Stake sidechains* [13] and *Proof-of-Work sidechains* [20].

Peer-based Systems enable users to exchange assets across distinct blockchains by participating in deals with other users. Peer-based systems exchange information by leveraging protocols that create agreements based on hashed timelock contracts (HTLCs). The systems that belong to this category are *Atomic Cross-Chain Swaps (ACCSs)* [15] and *Interledger* [16].

3 Evaluation Framework

In this section we propose an evaluation framework composed of five criteria to understand and analyze the architecture of cross-chain communication systems. We selected those five criteria because they are key components in the process of transporting and validating data and are therefore essential for establishing cross-chain communication.

The proposed evaluation framework serves as tool to provide a concise overview of the cross-chain communication capabilities of the selected systems and is composed by the following criteria:

Direction of communication defines in which direction cross-chain communication systems are able to transfer information. It can be either unidirectional or bidirectional. Systems with unidirectional data transfer only allow the destination chain to fetch data from the source chain, whereas systems with bidirectional data transfer enables both destination chain and source chain to send and receive data from each other.

Communication channel refers to the medium used to send the information required to execute the cross-chain operation. We divide a cross-chain operation into four phases: *setup*, *value transfer*, *claim transfer* and *settlement*.

The *setup* phase is used to exchange information regarding the structure of the deal such as intention to transfer, amount, addresses, conditions and time constraints. Those details should be analyzed when deciding whether to follow through with the deal or to abort the operation.

If participants agree on the parameters of the deal they move on to the *value transfer* phase. In this phase transactions are released to the counterparties or published in the blockchain. This may occur between multiple pairs of users (or hops) in scenarios where multiple participants route payments between blockchains along the way to a destination address.

After the involved parties execute their part of the deal, they enter the *claim transfer* phase, where a verifiable claim must be relayed to the counterparty in order to prove that an agreed upon action was performed and registered in the blockchain.

Finally, during the *settlement* phase, verifiable claims generated in the previous steps are validated and the final transaction in the cross-chain operation is committed to the blockchain, updating the state of the ledger. This may take from a few seconds to hours, depending on the confirmation latency of the involved blockchains. For each phase, one of the following channels can be used:

- *On-chain:* When a phase of the cross-chain operation takes place inside the blockchain, it is considered an on-chain communication.
- *Off-chain channels:* When a phase of the cross-chain operation takes place in a medium predefined by the protocol but is not recorded on the blockchain, we say it requires off-chain channels.
- *Out-of-bound channels:* When a phase of the cross-chain operation requires a communication channel that is not defined by the protocol (such as messaging apps, email, phone calls or in-person), it is considered an out-of-bound channel.

Type of Exchanged Information defines the type of data that can be sent across chains, including digital tokens and arbitrary data.

- *Digital token:* Digital tokens represent cryptocurrencies and are commonly represented as a key-value pair, where the key is the token address and the value is the amount of token balance (i.e., the number of tokens contained in that address) like in the UTXO model [25] or account model [7].
- *Arbitrary data:* Arbitrary data allows non-token data, such as the blockchain state, to be exchanged across chains. This is particularly useful for non-cryptocurrency blockchains, such as Hyperledger Fabric [2].

Verifiable Claims define how a blockchain system proves to another blockchain that an event, e.g., the acceptance of a transaction, has taken place. Events must be verified before committing operations to the blockchain in order to prevent malicious behavior. The verification of claims, as formally defined in a recent work [1], is a challenge for cross-chain communication mechanisms. A system can prove that data has been added to the chain through the following types of claims:

- *Validator signature:* A validator or set of validators are trusted to provide a proof about the internal state of a (commonly permissioned) blockchain. The proof could be in the form of a threshold number of signatures (or an aggregated signature to reduce the proof size) from the set of validators [1, 23, 36].
- *SPV proof:* Simplified Payment Verification (SPV) enables light clients (such as mobile wallets) to verify that a transaction has been included in the blockchain without downloading the entire blockchain history.
- *Pre-commitment:* A pre-commitment is a cryptographic construction which guarantees that a certain action, such as releasing a transaction, is going to be carried out once a condition is fulfilled. Pre-commitments are used to create agreements which prove that transactions are going to be released when all participants of the cross-chain operation commit to executing the deal.

Validator is the entity or group of entities responsible for verifying the validity of a verifiable claim generated in another blockchain. Validators may have elevated privileges, in which case the security of the system relies on the integrity of the set of validators, or may be selected in a trustless manner, leading consensus to be achieved when a majority of the blockchain users agree with the state changes proposed by the validator.

- *Permissionless validator:* We consider validators to be permissionless if they are (possibly weighted) randomly chosen from the set of blockchain participants. They are permissionless as any blockchain user can join the validation process. Systems that employ permissionless validators [7, 25, 29, 30] incentivize users to take part in the validation process through financial compensation.
- *Permissioned validator:* We consider validators to be permissioned if they are chosen from a fixed and pre-determined subset of blockchain participants. Unlike in permissionless systems, not every blockchain user can be a validator in a permissioned system.

4 Analysis

Distinct cross-chain communication systems achieve their objectives by employing mechanisms that differ in their levels of complexity. For that reason different cross-chain communication systems may present strengths and weakness when compared to each other. In this section we classify ten leading cross-chain communication systems (as presented in Table 1) according to our proposed evaluation framework. We also analyze the advantages and disadvantages of each proposed category of cross-chain communication systems using attributes based on those defined by the ISO/IEC 25010 software quality model [17]. Lastly, we provide a comparative analysis between the systems in each category. Rather than discussing the same set of properties for each analyzed system, we discuss only the unique properties that distinguish the systems apart from each other.

Table 1. Classification of cross-chain communication systems.

System attributes		Blockchain Ecosystems		Relay-based systems			Sidechain-based systems			Peer-based systems	
		Cosmos	Polkadot	BTC Relay	ETH Relay	Proof-of-Burn	Liquid Network	PoS Sidechains	PoW Sidechains	Atomic Swaps	Interledger
Direction of communication	Unidirectional			X	X	X					
	Bidirectional	X	X				X	X	X	X	X
Communication Channel*	Setup	●	●	●	●	●	◐	●	●	○	◐
	Value transfer	●	●	●	●	●	●	●	●	●	○
	Claim transfer	●	●	○	○	○	◐	●	○	○	○
	Settlement	●	●	●	●	●	●	●	●	●	●
Verifiable Claims	Validator signature		X				X	X			
	SPV proof	X		X	X	X			X		
	Pre-commitment									X	X
Validator	Permissionless		X	X	X			X	X		
	Permissioned						X				
	Blockchain dependent	X				X				X	X
Type of exchanged information	Digital tokens	X	X	X	X	X	X	X	X	X	X
	Arbitrary data	X	X					X	X		

* On-Chain: ●; Off-Chain: ◐; Out-of-Bounds: ○.

4.1 Blockchain Ecosystems

Blockchain ecosystems (illustrated in Fig. 1) are networks that host independent interconnected blockchains. Ecosystems are organized in a topology in which multiple blockchains are connected to one central blockchain. The central blockchain serves as a connector that forwards information across connected blockchains (a.k.a. internal blockchains). Internal blockchains can also establish communication with external chains, i.e., those not deployed inside the ecosystem.

However, this requires the development of bridging systems to adapt the information coming from external chains in such a way that it can be understood by the internal chains.

- **Strengths:**
  Compatibility (Interoperability): Internal chains can participate in cross-chain operations with other internal chains connected to the central chain without requiring adaptations or additional configuration.

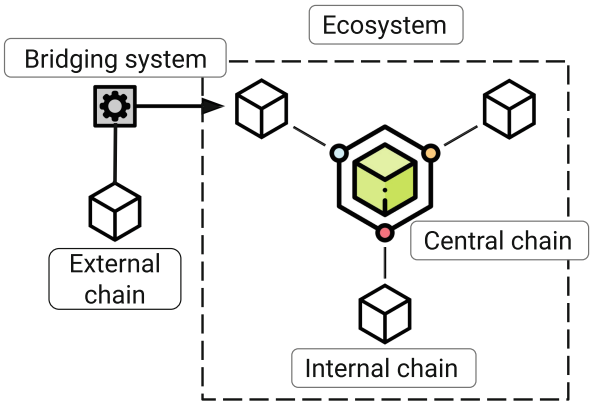

Fig. 1. Architectural overview of blockchain ecosystems.

- **Weaknesses:**
  Portability (Installability): Developing and deploying a blockchain inside an ecosystem is hard and time consuming. Blockchains need to be compatible with the requirements of the ecosystem, e.g., a specific consensus engine. In order to deploy blockchains inside an ecosystem as an internal chain, aspects such as block proposal strategy, validation incentives and feature support might need to reconsidered.
  Portability (Adaptability): Blockchains deployed inside an ecosystem only natively support communication with other internal chains. If communication with an external chain is needed, a bridging system is required.

Cosmos is an ecosystem of interconnected independent blockchains. In Cosmos, there are zones and hubs. Zones are regular blockchains but can also choose to become hubs, which are a special type of blockchains that connects zones together. Zones can communicate with a theoretically unlimited number of other zones as long as they are connected to a common hub. The Cosmos ecosystem is permissionless, allowing anyone to deploy a blockchain in the network. Zones are powered by Tendermint BFT[1]. Cosmos has a native token called ATOM, which is used to secure the Cosmos Hub through a staking-based validator selection process.

Polkadot is a network of interconnected blockchains. In the network there are multiple parachains and one relay-chain. Parachains are independent blockchains that run in parallel and the relay-chain is a central chain that validates blocks proposed by the parachains and coordinates the entire network. The relay-chain provides a shared view of every parachain's state to the ecosystem. Polkadot has a native token that is used for staking, called the DOT. Staking DOTs is

[1] https://tendermint.com/core/.

a requirement for being a relay-chain validator and is also required for joining the auction process that leases parachain slots in the network. Polkadot provides a protocol called Cross-Chain Message Passing (XCMP) to enable the transfer of assets and arbitrary data between parachains. Parachains need to open one channel for sending messages and another one for receiving messages for each parachain they want to communicate with. Those channels require funding using DOT tokens, which are returned when the channels are closed[2].

Analysis of Blockchain Ecosystems. The two well-known systems in this category are Cosmos and Polkadot. Both systems aim to reduce the difficulty and time required to develop and deploy blockchains inside their networks by providing frameworks for blockchain development. Cosmos offers the Cosmos SDK and Polkadot offers the Substrate framework. Both are modular frameworks that provide developers with pre-built modules that can be applied to blockchains, eliminating the need for designing basic functionalities such as governance, staking and token distribution.

Polkadot offers a limited number of 100 slots in which parachains can be deployed[3]. Consequently, users are required to participate in an auction process to earn the right to deploy their blockchain inside the ecosystem. This makes it unlikely for small companies and blockchain projects to secure a slot in the network due to the requirement of competing in an auction against well-funded companies and projects. Cosmos in comparison, offers unlimited slots, allowing anyone to create a zone in the network without any barriers to entry.

When it comes to block production, Cosmos zones are responsible for selecting their own set of validators and achieving block finality through Tendermint consensus. Hubs are not responsible for validating transactions issued in the zones connected to it [22]. Parachains, on the other hand, are responsible for determining their own block production strategy, carried out by participants called collators, but cannot validate blocks on their own. Blocks proposed by collators must be approved by a global set of relay-chain validators that are responsible for guaranteeing the security of the entire ecosystem. Relay-chain validators are assigned to parachains in a rotating fashion and perform the validation of proposed blocks before adding them to the ecosystem's relay-chain. As both ecosystems rely on strategies that require a pre-defined set of validators to approve and finalize blocks, they are incompatible with blockchains that employ Proof-of-Work (PoW) based consensus.

Validation is performed locally in Cosmos zones and globally in Polkadot's parachains, therefore their security assumptions differ. The Polkadot network is secured by a large amount of tokens staked by system wide relay-chain validators. In Cosmos, every zone is responsible for maintaining its own state and keeping it secure through their own individual staking process. This means that during cross-chain communication, Cosmos zones need to trust other zones they are interacting with. In Polkadot, parachain's states are shared across the entire

[2] https://wiki.polkadot.network/docs/en/learn-crosschain.
[3] https://wiki.polkadot.network/docs/en/learn-auction.

ecosystem through the relay-chain, therefore, trust assumptions are on the relay-chain's validators rather than in the individual parachains. As a consequence of Cosmos' security model, zones with a small amount of staked tokens are more susceptible to attacks when compared to Polkadot's parachains, which are secured by large amounts of staked tokens. If an attacker is able to acquire the majority of the stake in a zone she can influence the outcome of governance proposals and selectively censor transactions.

4.2 Relay-Based Systems

Relay-based systems (illustrated in Fig. 2) enable information about state changes in one source blockchain to be relayed to and validated inside one destination blockchain using a smart contract. This information can be used for asset exchange and asset portability [6]. This process does not require the source chain to have any knowledge of the relay contract. The communication provided by relay systems is unidirectional, if a party needs to fetch information bidirectionally, two independent relay systems must be used.

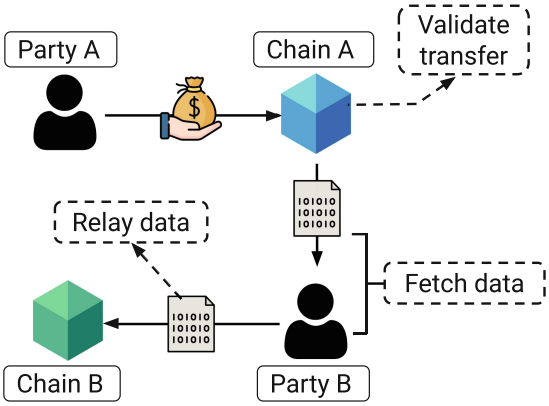

Fig. 2. Overview of asset transfer using a relay-based system.

- **Strengths:**
  Portability (Installability): Relays can be implemented in a destination chain without requiring the source chain to have any knowledge of it.
- **Weaknesses:**
  Performance efficiency (Resource utilization): As smart contracts are leveraged for transaction validation, the cost of verifying data using relay-based systems is proportional to the complexity of the verification algorithm.
  Security (Integrity): Relay-based systems are susceptible to block reorganization attacks. Most relay solutions [8,11,26] only work with source chains that achieve probabilistic block finality and those chains may have their blocks reorganized after suffering an attack, invalidating a previously accepted transaction.

BTC Relay is a system that enables information to be relayed from the Bitcoin to the Ethereum blockchain and allows users to validate this information on Ethereum. BTC Relay receives and stores on the Ethereum blockchain the Bitcoin block information relayed by users. The system charges a fee to validate the received block information according to Bitcoin's consensus algorithm. BTC Relay allows Ethereum to verify and react to the state of Bitcoin's blockchain but not the other way around. No action needs to be taken the Bitcoin blockchain for block information to be relayed neither for it to be verified in Ethereum.

ETH Relay can be deployed in a destination chain to validate block information coming from a source chain in a cost-effective way. This system allows any pair of Ethereum-based blockchains to establish cross-chain communication but only works unidirectionally.

ETH Relay uses an optimistic way of accepting block headers, accepting them without validation at first, but keeping them on a trial period in which users can dispute its validity. ETH Relay also enables efficient transaction verification by storing information about block branches and paths along with block headers, allowing the system to traverse blockchain data in an efficient way.

Proof-of-Burn is a mechanism that allows tokens to be transferred across blockchains by destroying them in a source chain, verifying the operation in a destination chain and then generating a representation of the destroyed assets.

To transfer asset using Proof-of-Burn, digital assets must first be "burned" in the source chain. In order to do that, users need to send the assets to a provably non-spendable wallet address causing them to be lost forever. To verify that the burning transaction has been committed in the source chain, a proof of inclusion has to be relayed to the destination chain. This proof needs to be verified in a smart contract prior to creating new assets. The burning procedure is unidirectional, can only be conducted once and is irreversible once the assets have been transferred to a burn (non-spendable) address.

Analysis of Relay-Based Systems. The relay-based systems category includes BTC Relay, ETH Relay and Proof-of-Burn. Both BTC Relay and ETH Relay serve the same purpose, which is to allow a destination chain to verify state changes in a source chain. In terms of adaptability, however, BTC Relay is limited to verifying Bitcoin state changes inside the Ethereum blockchain, whereas ETH Relay can be applied to any pair of Ethereum-based blockchains. In addition, ETH Relay is more cost-effective than BTC Relay as it employs a block validation strategy that is optimized to consume less computational resources.

Proof-of-Burn on the other hand, was not idealized as a cross-chain communication system, but as a way to burn currency in exchange for participating in the block validation process. Burned assets are lost forever, potentially causing problems such as inflation due to reduction in asset availability if many burning operations are executed. However, while not ideal for simple cross-chain asset

transfers, Proof-of-Burn fits niche use-cases such as being used for destroying one type of token in order to transfer value to a different digital asset in a different blockchain [18]. This system should be used cautiously as destroying assets without having a guaranteed way of claiming them in another blockchain may lead to losing them forever. Additionally, if the burn operation is not set up in a secure and verifiable manner, burned assets may be claimed multiple times inside distinct blockchains as the claim remains unknown to other ledgers.

4.3 Sidechain-Based Systems

A sidechain is a blockchain that is connected to another ledger referred to as the main chain through a mechanism that enables assets to be transferred back and forth between both blockchains. The mechanism which allows a sidechain and main chain to communicate bidirectionally is called a two-way peg, thus connected blockchains are also referred to as pegged chains. Sidechain systems must be adapted to a specific pair of blockchains. Figure 3 presents a generalization of the architecture and communication between pegged chains.

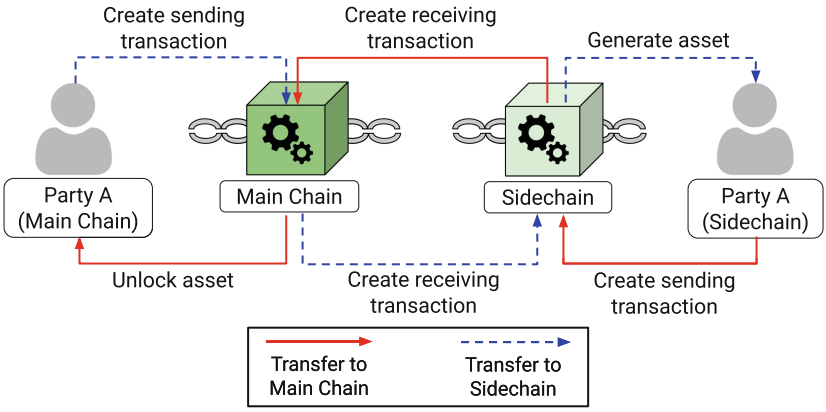

Fig. 3. Transfer of assets between sidechains.

The relationship between a sidechain and a main chain can be either symmetric or asymmetric. When symmetric, both chains are able to operate independently and failure in one of them does not directly affect the other. Nodes in the main chain do not have to be aware of the sidechain and vice-versa, unless they want to actively take part in cross-chain operations [20]. The asymmetric scheme consists of an independent main blockchain and a sidechain that relies on the main chain to operate. All the sidechain nodes are aware of the main chain, however, only main chain nodes who chose to support the sidechain are aware of it. When chains have an asymmetric relationship, failures on the main chain will have an impact on the sidechain, the opposite, however, is not true.

- **Strengths:**
  Maintainability (Modifiability): A benefit of sidechains is the possibility to extend blockchain functionality. Connecting a sidechain to a main chain that is deprived of certain features, e.g., transaction privacy, can enable users of said main chain to have access to additional desirable features without requiring changes in the main chain.
- **Weaknesses:**
  Portability (Installability): Sidechains systems must be developed for a specific pair of blockchains and therefore need to be designed to be compatible with both chains before deployment. Sidechains can also increase the complexity of a system in different levels [3].
  Decentralization: Sidechains are susceptible to centralization of mining when one of the connected chains provides higher mining incentives than the other. This leads miners to work only for the most profitable chain and may slow down block validation in the other chain.

Liquid Network is a federated sidechain that allows assets to be moved from the Bitcoin blockchain and back to it. When assets are moved to the sidechain they fall under custody of a group of participants called functionaries [9]. Bitcoins (BTC) transferred to Liquid are represented as Liquid Bitcoins (L-BTC) inside the sidechain. For every existing amount of L-BTC there has to be a correspondent amount of BTC locked in the Bitcoin blockchain.

Proof-of-Stake Sidechains are sidechain constructions that enable cross-chain communication between Proof-of-Stake (PoS) blockchains. To transfer assets users must diffuse a message signaling their intention to transfer assets to the other chain in the source chain and a recovery message to reclaim its assets on the destination chain. The same operation can then be conducted in the sidechain to transfer the assets back to their source chain. Cross-chain proofs require a signature from a set of validators chosen through a leader election algorithm.

Proof-of-Work Sidechains are sidechain constructions that enable two independent Proof-of-Work based chains to establish cross-chain communication. To prove that an event took place in another chain, the proposed construction uses a cryptographic proof of state called Non-Interactive Proofs of Proof-of-Work (NIPoPoWs) [19]. The use of Proof-of-Work makes this system trustless, as users don't have to trust other peers, but rather validate transactions through a decentralized consensus algorithm. This system has the ability to transfer arbitrary data between chains in addition to transferring digital tokens.

Analysis of Sidechain-Based Systems. The sidechain-based systems category main contains three cross-chain communication systems, namely Liquid Network, Proof-of-Stake sidechains and Proof-of-Work sidechains. Out of all three, the Liquid Network is the most limited in terms of adaptability, being

restricted to cross-chain operations between the Bitcoin and the Liquid Network blockchains. Proof-of-Stake and Proof-of-Work sidechains are generic constructions and therefore can be incorporated to any Proof-of-stake and Proof-of-Work based blockchains respectively.

In regards to ease of use, the Liquid Network has an advantage over the other systems in this category. This is due to the fact that Liquid is a sidechain solution that has already been deployed, eliminating the need for development and deployment work. All one needs to start using Liquid is to transfer BTC to a Liquid Network peg-in address to receive an equivalent amount of L-BTC in the sidechain. The Liquid sidechain also provides features not available within the Bitcoin blockchain and makes them accessible via the use of BTC. Those features include fast transaction speed, enhanced transaction privacy and the ability for users to issue their own tokens. On the other hand, Proof-of-Stake and Proof-of-Work sidechains are academic proposals that require considerable effort to be developed into fully functioning sidechains, given that their objective is to provide generic constructions to enable secure cross-chain communication. However, despite not being ready-to-use systems like the Liquid Network, Proof-of-Stake and Proof-of-Work sidechains provide rigorously defined constructions that can be used as a reference for the development of cross-chain communication mechanisms from scratch while enabling developers to design the remaining sidechain components in a way that suits their needs.

In terms of consensus, Proof-of-Stake and Proof-of-Work sidechains were designed to work with blockchains that employ those specific consensus mechanisms and therefore are better tailored for a permissionless setting. The Liquid Network operates under a federated model and relies on a set of pre-defined validators called functionaries to secure the network. When users exchange their BTC for L-BTC, their BTC fall under control of Liquid's functionaries, requiring users to trust that the federation will keep their locked assets secure. The use of federations is a trade-off of decentralization for faster transaction processing speed.

4.4 Peer-Based Systems

Peer-based systems allow users to exchange assets directly with other peers rather than relying on a third party service. Figure 4 presents a generalization of the process of transferring assets using peer-based systems.

User-to-user communication in peer-based systems takes place in communication channels outside of the blockchain environment. To enforce correctness and security during transfers, this category of systems relies on protocols that employ HTLCs and pre-commitments to coordinate the transfer of value across chains. Those systems allow two parties in any two different blockchains to engage in cross-chain asset transfer, as long as both blockchains support the scripting capabilities necessary to set up the exchange contracts.

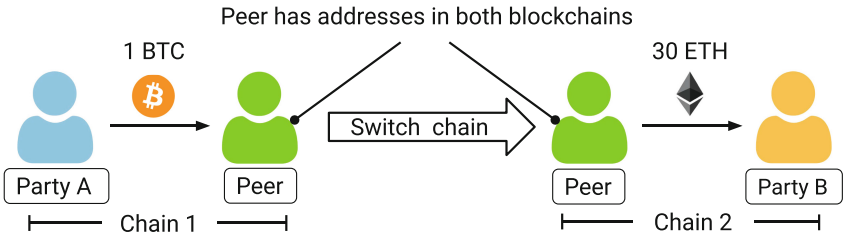

Fig. 4. Process of transferring assets using peer-based systems.

- **Strengths:**
  Portability (Installability): Transfers that leverage peers to forward assets across systems can be executed without the need to deploy complex systems. Setting up the exchange contracts requires less time and effort than deploying other types of cross-chain communication systems such as sidechains and relay contracts.
- **Weaknesses:**
  Performance efficiency (Time behaviour): Settlement of transactions using peer-based systems can have long delays. Those delays are caused by the hashed timelock contracts (HTLCs) and the time required to allow parties to participate in or to abort deals.

Atomic Cross-Chain Swaps (ACCSs) allow users to participate in atomic asset exchanges between blockchains. A swap takes place between parties who hold assets in distinct blockchains, however, users must also have an account or address in the blockchain on which they wish to receive their payment. For example, if Alice wants to exchange BTC for Ether and Bob wants to exchange Ether for BTC, both parties need one address in each participating blockchain to be able to execute a swap.

To set up a deal using ACCSs, the participants must establish an out-of-bounds communication channel to agree on the details of the operation. The asset transfer protocol is coordinated using HTLCs, which carry out actions when the conditions agreed upon by the participants of the deal are met.

Interledger is a protocol suite that allows users in independent blockchains to exchange assets through a payment routing network composed of other users. Interledger is optimized for the transfer of micro payments, making it similar to payment channels. It can be used by anyone without requiring any development or deployment process.

When a user wishes to transfer assets, the Interledger protocol is used to find a route of connected users that can form a path to forward the value packets hop by hop from the sender to the receiver, across different blockchains. Users that connect other peers in the network can earn revenue by taking margins from the transfers they aid in. Whenever a user wishes to forward payments to a different peer, a route of connectors between them must be established before sending value.

Analysis of Peer-Based Systems. The peer-based systems category includes Atomic Cross-chain Swaps and Interledger. Those systems require no development effort in order to be used for cross-chain communication. ACCSs are coordinated using HTLCs and while they require programming knowledge to set up, the effort required is smaller than the effort needed to develop a full-fledged cross-chain communication system. Interledger utilizes the Interledger Protocol to find routes of peers to connect the users that want to exchange payments. All one needs to use Interledger is to use the protocol to find a suitable route of peers through which value packets can be forwarded. Even though fairness issues have been identified in the Atomic Cross-chain Swap protocol and patched [14], in general peer-based systems are secure and enforce correctness of transactions, meaning that users obtain what they expect.

Neither ACCSs or Interledger are tied to specific blockchains, however ACCSs require the ledgers involved in the cross-chain operation to support the creation of HTLCs. Interledger uses hashed timelock agreements (HTLAs), a generalization of HTLCs that can be implemented in any type of blockchain. Additionally, Interledger can also be used to exchange value with fiat money payment networks, a feature that is not supported by ACCSs.

Functional suitability however, is where the two systems differ. ACCSs only allow the execution of one cross-chain deal and need to be set up every time assets need to be transferred across blockchains. Additionally, operations using ACCSs take a long time (can last for 48 h) and users need to stay active throughout the execution of the protocol in order to claim their assets. In contrast, Interledger is optimized for micropayments and allows users to open payments channels with each other and exchange value packets until one of the parties wishes to close the channel and update their balance in the blockchain. This characteristic makes Interledger more suitable for users that need to execute large volumes of small value transactions over a long period of time.

5 Related Work

Since works proposing systems to achieve cross-chain communication in specific scenarios were discussed and analyzed in detail throughout this work, we limit the related work discussion to relevant literature that approaches the problem of cross-chain communication from a broader, more general perspective.

Zamyatin et al. provides a systematic analysis of existing blockchain protocols and formalizes the problem of Cross-Chain Communication [37]. The authors draw a comparison between the process of establishing cross-chain communication and the Fair Exchange problem, arguing that cross-chain communication is impossible without the help of a trusted third party. This work also presents a framework for analyzing blockchain interoperability solutions and uses it to classify existing protocols.

Buterin presents a preliminary view of the blockchain interoperability field, classifies existing solutions into distinct categories and discusses expectations for the future of cross-chain communication [6].

Belchior et al. conducts an extensive literature review on blockchain interoperability [4]. The authors review and classify blockchain interoperability systems and provide up-to-date information on grey literature.

Frauenthaler et al. analyzes the blockchain literature and proposes technical criteria to classify existing work [12]. The authors also define core principles required for achieving interoperability.

Lohachab et al. presents a systematic review of blockchain interoperability and its different aspects, requirements and implementations [24]. The authors propose a taxonomy for blockchain research and a multi-layer architecture to achieve interoperability among heterogeneous blockchains.

6 Conclusion

With the increased interest in blockchain technologies cross-chain communication is more desired than ever. This work provided a study on the architecture of cross-chain communication systems with the aim of expanding the knowledge on the subject and supporting developers and practitioners in the process of selecting cross-chain communication systems suitable for their needs. We hope the community can benefit from our proposed evaluation framework, which provides a concise way of assessing the capabilities of interoperability systems, and our analysis, which provides support in the process of weighing the benefits and drawbacks of existing systems and their respective categories.

References

1. Abebe, E., et al.: Verifiable observation of permissioned ledgers (2020)
2. Androulaki, E., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, pp. 1–15 (2018)
3. Back, A., et al.: Enabling blockchain innovations with pegged sidechains (2014)
4. Belchior, R., Vasconcelos, A., Guerreiro, S., Correia, M.: A survey on blockchain interoperability: past, present, and future trends. arXiv preprint (2020)
5. Burdges, J., et al.: Overview of polkadot and its design considerations. arXiv preprint (2020)
6. Buterin, V.: Chain interoperability. R3 Research Paper (2016)
7. Buterin, V.: Ethereum whitepaper (2021). https://ethereum.org/en/whitepaper/
8. Consensys: BTC Relay. https://github.com/ethereum/btcrelay
9. Dilley, J., Poelstra, A., Wilkins, J., Piekarska, M., Gorlick, B., Friedenbach, M.: Strong federations: an interoperable blockchain solution to centralized third-party risks. arXiv (2016)
10. Dujak, D., Sajter, D.: Blockchain applications in supply chain. In: Kawa, A., Maryniak, A. (eds.) SMART Supply Network. E, pp. 21–46. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-91668-2_2
11. Frauenthaler, P., Sigwart, M., Spanring, C., Sober, M., Schulte, S.: Eth relay: a cost-efficient relay for ethereum-based blockchains. In: 2020 IEEE International Conference on Blockchain (Blockchain), pp. 204–213 (2020)

12. Frauenthaler, P., Borkowski, M., Schulte, S.: A framework for blockchain interoperability and runtime selection. arXiv preprint arXiv:1905.07014 (2019)
13. Gazi, P., Kiayias, A., Zindros, D.: Proof-of-stake sidechains. IACR Cryptology ePrint Archive 2018/1239 (2018)
14. Han, R., Lin, H., Yu, J.: On the optionality and fairness of atomic swaps. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, 21–23 October 2019, pp. 62–75 (2019)
15. Herlihy, M.: Atomic cross-chain swaps. In: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, pp. 245–254 (2018)
16. Interledger Foundation: Interledger protocol v4. https://tinyurl.com/2aj635xm
17. ISO/IEC 25010: System and software quality requirements and evaluation. Technical report, International Organization for Standardization
18. Karantias, K., Kiayias, A., Zindros, D.: Proof-of-burn. IACR Crypto (2019)
19. Kiayias, A., Miller, A., Zindros, D.: Non-interactive proofs of proof-of-work. IACR Crypto **2017**(963), 1–42 (2017)
20. Kiayias, A., Zindros, D.: Proof-of-work sidechains. In: Bracciali, A., Clark, J., Pintore, F., Rønne, P.B., Sala, M. (eds.) FC 2019. LNCS, vol. 11599, pp. 21–34. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-43725-1_3
21. Kuo, T.T., Kim, H.E., Ohno-Machado, L.: Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. **24**(6), 1211–1220 (2017)
22. Kwon, J., Buchman, E.: Cosmos whitepaper (2019)
23. Le, D.P., Yang, G., Ghorbani, A.: A new multisignature scheme with public key aggregation for blockchain. In: 2019 17th PST, pp. 1–7. IEEE (2019)
24. Lohachab, A., et al.: Towards interconnected blockchains: a comprehensive review of the role of interoperability among disparate blockchains. ACM Comput. Surv. (CSUR) **54**(7), 1–39 (2021)
25. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
26. Network, K.: Peace Relay. https://github.com/KyberNetwork/peace-relay
27. Nick, J., Poelstra, A., Sanders, G.: Liquid: a bitcoin sidechain (2020)
28. Pilkington, M.: Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations. Edward Elgar Publishing (2016)
29. Project, T.M.: About monero (2021). https://www.getmonero.org/resources/about/
30. Sasson, E.B., et al.: Zerocash: decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy, pp. 459–474. IEEE (2014)
31. Sekniqi, K., Laine, D., Buttolph, S., Sirer, E.: Avalanche platform (2020)
32. Tasatanattakool, P., Techapanupreeda, C.: Blockchain: challenges and applications. In: ICOIN 2018, pp. 473–475. IEEE (2018)
33. Tether Operations: Tether cryptocurrency (2021). https://tether.to/
34. Vilner, Y.: New report illustrates the problem with cryptocurrency exchanges, June 2019. https://tinyurl.com/ad9djc6e
35. Wood, G.: Polkadot: vision for a heterogeneous multi-chain framework (2016)
36. Xiao, Y., Zhang, P., Liu, Y.: Secure and efficient multi-signature schemes for fabric: an enterprise blockchain platform. IEEE Trans. Inf. Forensics Secur. **16**, 1782–1794 (2020)
37. Zamyatin, A., et al.: SoK: communication across distributed ledgers (2019)
38. Zamyatin, A., Harz, D., Lind, J., Panayiotou, P., Gervais, A., Knottenbelt, W.: XCLAIM: trustless, interoperable, cryptocurrency-backed assets. In: 2019 IEEE Symposium on Security and Privacy (SP), pp. 193–210. IEEE (2019)
39. Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**(4), 352–375 (2018)