Received: 18 October 2022 | Revised: 8 January 2023 | Accepted: 10 February 2023

DOI: 10.1049/cmu2.12594

IET Communications

The Institution of Engineering and Technology WILEY

REVIEW

Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication

Seth Djanie Kotey[1,2] | Eric Tutu Tchao[1,2] | Abdul-Rahman Ahmed[1,3] | Andrew Selasi Agbemenu[1,2] | Henry Nunoo-Mensah[1,2] | Axel Sikora[4] | Dominik Welte[4] | Eliel Keelson[1,2]

[1]Distributed IoT Platforms, Privacy and Edge-Intelligence Research (DIPPER) Laboratory, Faculty of Electrical and Computer Engineering, Kwame Nkrumah University of Science and Technology, Ghana

[2]Department of Computer Engineering, Kwame Nkrumah University of Science and Technology, Ghana

[3]Department of Telecommunications Engineering, Kwame Nkrumah University of Science and Technology, Ghana

[4]Institute Reliable Embedded Systems and Communication Electronics, University of Applied Sciences, Offenburg, Germany

Correspondence
Seth Djanie Kotey, Eric Tutu Tchao, Distributed IoT Platforms, Privacy and Edge-Intelligence Research (DIPPER) Laboratory, Faculty of Electrical and Computer Engineering, Kwame Nkrumah University of Science and Technology, Ghana.
Email: kotey.seth11@gmail.com; ettchao.coe.coe@knust.edu.gh

Funding information
BMBF, Grant/Award Number: 01DG21017; DAAD, Grant/Award Number: 57557211

Abstract

Blockchain technology has been increasingly adopted over the past few years since the introduction of Bitcoin, with several blockchain architectures and solutions being proposed. Most proposed solutions have been developed in isolation, without a standard protocol or cryptographic structure to work with. This has led to the problem of interoperability, where solutions running on different blockchain platforms are unable to communicate, limiting the scope of use. With blockchains being adopted in a variety of fields such as the Internet of Things, it is expected that the problem of interoperability if not addressed quickly, will stifle technology advancement. This paper presents the current state of interoperability solutions proposed for heterogenous blockchain systems. A look is taken at interoperability solutions, not only for cryptocurrencies, but also for general data-based use cases. Current open issues in heterogenous blockchain interoperability are presented. Additionally, some possible research directions are presented to enhance and to extend the existing blockchain interoperability solutions. It was discovered that though there are a number of proposed solutions in literature, few have seen real-world implementation. The lack of blockchain-specific standards has slowed the progress of interoperability. It was also realized that most of the proposed solutions are developed targeting cryptocurrency-based applications.

1 | INTRODUCTION

Blockchain is a technology originally developed to allow for collaborators to easily certify when a document was created or last modified [1]. Blockchain and other distributed ledgers were developed to be used as tamper-evident logs for recording data, with modifications to the ledger recorded as separate events in an append-only fashion. This append-only method gives blockchain its immutability property, and it relies on cryptographical methods to ensure this immutability as well as verifiability of data [2].

The Bitcoin whitepaper [3] released in 2008 established a working model for blockchain, and spurred interest in the blockchain technology. Blockchain was initially thought of as technology to disrupt the centralized banking system [4], however, it is now seen as a technology with more potential use cases. This can be attributed to the success of Bitcoin. Currently, blockchain is seen as a technology to further advance data storage and record keeping in different fields [5], including supply chains, Industrial Internet of Things [6], healthcare, logistics, manufacturing, energy [7, 8], and is seeing a rapid increase in adoption in these fields. Its ledger-based design [9] ensures that data can only be appended, which provides a full transactional history. Appending data to the ledger among untrusted nodes is done through consensus [10], a transformation of the Byzantine General's Problem [11], to ensure the most trustworthy data is added to the blockchain.

The adoption of blockchain in industries has the potential to transform how data is processed and offered. Data availability, integrity, transparency, traceability and auditability are important properties for data processing in industrial processes [12], and with blockchain offering these properties [7], industries are looking to adopt the technology to improve data handling. The Internet of Things (IoT) in industries in particular has experienced rapid growth [13]. IoT devices generate a lot of very important data to help industries in their processes. IoT has benefitted industries to a large extent, however, the centralized architecture on which it is built [14] has led to the integration of blockchain with IoT [15]. Fields in which blockchain has been integrated with IoT include: Supply Chains [16, 17], Healthcare [18–20] and Smart Cities [21, 22].

The rapid development of blockchain has brought into existence various protocols and architectures for developing blockchain solutions. The lack of blockchain architecture-specific standards means there is no standard protocol or cryptographic structure developers work with in developing new blockchain architectures [23]. This has made blockchains like walled gardens [24], without the ability of information to be easily exchanged between two different blockchains [25]. The development of distinct and incompatible blockchains [26] has created significant division in research, and this has led to many blockchains which are isolated from each other. As the adoption of blockchain increases in various fields, interoperability between the different blockchain architectures being proposed is a major topic for discussion [27]. This is important especially for collaborating organizations.

Currently, blockchains can be either public, private or hybrid, and different implementations have been proposed under each category. Each of these categories has their advantages and disadvantages and the decision to select one or the other is dependent on the requirements of the particular organization. This may cause different organizations working together to adopt different blockchains for their operations based on their organizational requirements. As the different organizations use different blockchains to meet their organizational needs, a new problem is created when there needs to be collaboration between these organizations using different blockchains; how to interoperate these different blockchains.

Contextually, blockchain interoperability means connecting multiple blockchains to access information and to act on the information. It requires that either assets can be transferred from one blockchain to another blockchain or that the users are capable of accessing information on one blockchain while on another blockchain, where blockchain assets could either be cryptocurrency or data. Blockchain interoperability enables a secure transition of state information between different blockchains, and this would enable the creation of transmission routes for connecting the decentralized internet (Web3.0) [28].

This paper therefore seeks to provide an overview of the interoperability solutions for heterogenous blockchains which have been proposed. The paper makes the following contributions:

- A systematic review of the current state-of-the-art in heterogenous blockchain interoperability is presented, discussing their pros, cons and target domains.
- Proposed interoperability solutions reviewed are compared based on six criteria.
- Open issues on the current state of blockchain interoperability are discussed and research directions to aid in research efforts are presented.
- A taxonomy for classifying the current state-of-the-art heterogenous blockchain interoperability solutions is presented.

The rest of the paper is organized as follows: Section 2 presents related literature reviews and the review methodology is described in Section 3. Section 4 contains information on the State of the Art. The solutions are compared and discussed in Section 5, Open Issues and Research Directions are presented in Section 6, and the paper is concluded in Section 7. For ease of communication, 'blockchain' and 'chain' will be used interchangeably in this paper.

2 | RELATED LITERATURE REVIEWS

The growth of blockchain technology has revealed the problem of interoperability in the blockchain field. A lot blockchain proposals have been made in isolation, and this has led to studies being done to tackle the problem of interoperability. Several literature surveys have been conducted to present the proposed solutions tackling the problem of interoperability and in this chapter, some of these literature surveys are presented.

Qasse et al. [29] presented a survey on inter blockchain communication. In their paper, they discussed the existing cross blockchain communication solutions and grouped them under four categories: Sidechains, Blockchain Routers, Industrial solutions and Smart Contract-based solutions. Sidechain solutions are described as an approach utilizing a two-way peg for communication. Blockchain routers have some nodes acting as routers to transmit requests between blockchains. Industrial solutions use a set of trusted validators to validate transactions across blockchains and smart contract-based solutions use smart contracts to create interoperable protocols between the different blockchains. Their review focused on homogenous blockchain communication, indicating a focus on heterogenous blockchain communication needs a few more years to be developed.

Mohanty et al. [30] presented a study on blockchain interoperability with a focus on atomic-swap protocols. They categorized the solutions under Sidechains, Notary schemes, Blockchain Routers, Industrial Solutions and Hashed Time Locks and briefly mentioned some solutions under these categories. They further discussed atomic swaps in detail and discussed some proposed atomic swap protocols and their shortcomings. They proposed some future research directions to improve on atomic cross-chain swap protocols.

Monika and Bhatia [31] presented a survey of interoperability solutions provided by both the research community and industry. They presented the solutions under: Notary schemes, Sidechain/Relay solutions, Bridging Solutions, Smart Contract solutions, and Blockchain router solutions. They briefly described the solutions presented under the stated categories; however, some solutions seem to have been miscategorized, with the likely cause due to very little information in literature about those solutions. They further mentioned the disadvantages of each of the blockchain solution categories they mentioned.

Belchior et al. [32] presented a survey on blockchain interoperability. They categorized works under Public Connectors, Hybrid Connectors and Blockchain of Blockchains. They proposed a Blockchain Interoperability Framework which defines a set of criteria for assessing blockchain interoperability solutions. They identified potential use cases that could gain from the multi-blockchain approach and the challenges associated with developing blockchain interoperability solutions. The realized that the blockchain interoperability solution would benefit a wider array of applications and not only cryptocurrencies. Finally, they presented research directions based on the categories, architectures and supporting technologies of blockchain interoperability.

Johnson et al. [33] presented a review on interoperability and sidechains. Sidechains as they described it for their review refers to a sub-chain which takes traffic of a main public chain, which in some literature is referred to as a sub-chain or satellite chain. They presented a summary of sidechain projects including an Ethereum Private Sidechain project by ConsenSys [34], Plasma and Polkadot's parachains and relay chain concept. They also discussed sharding in Ethereum as well as some other blockchain interoperability solutions. For the solutions they reviewed however, most sought to create interoperability between chains running on the same blockchain platform.

Schulte et al. [35] discussed the need for interoperating blockchains whilst also presenting some interoperability solutions. They discussed blockchain interoperability from two perspectives; Cross-Blockchain Token Transfers and Cross-Blockchain Smart Contract Interaction. They described Cross-Blockchain Token Transfers as methods which involve the transfer of tokens like cryptocurrency coins from one blockchain to another. Cross-Blockchain Smart Contract Interaction was described as the method of invoking smart contracts to run on different blockchains. Research directions were also discussed for each of the blockchain interoperability perspectives they mentioned.

Khan et al. [36] provided an overview of the role of smart contracts in blockchain interoperability. They described how smart contracts are used in blockchains. They discussed the use of smart contracts between both homogenous and heterogenous blockchains. They further specified some of the ways in which smart contracts are applied in interoperability, for example using time lock contracts, relay smart contracts, off-chain smart contracts, bridge contracts and smart contract invocation methods, whilst differentiating between methods use for homogenous and heterogenous blockchains. They went further to provide some challenges and future directions for blockchain interoperability.

Velloso et al. [37] presented a review of solutions to enable cross-blockchain communication. They presented the main issues surrounding blockchain interoperability and the approaches to solve these issues. They discussed multi-blockchain systems under three categories; hierarchical blockchains, shard blockchains and sidechains. Hierarchical blockchains were described as large blockchains which have been subdivided into several smaller ones, with each subdivision associated with a level to provide hierarchy. Shard blockchains were described as large blockchains divided into smaller ones with no form of hierarchy. Sidechains were described as independent blockchains connected to a main blockchain. Some industry solutions for cross-chain communication were also mentioned, but were not categorized. The main focus of the review was centred around applying blockchain technology to secure virtual machine migration.

Talib et al. [38] presented a systematic review of solutions to enable blockchain interoperability. They examined the methodologies used in developing the solutions and the performance metrics used to benchmark the solutions. They discussed solutions based on four categories; Sidechain/relays, blockchain routers, smart contracts and industrial solutions. Atomic cross-chain swaps were also mentioned in their review. They presented inter-blockchain application areas based on the solutions reviewed and concluded with future research directions for the scientific community.

Qasse et al. presented blockchain interoperability solutions and mentioned a few research general directions without discussing them in detail. Mohanty et al. provided an overview of blockchain interoperability solutions and focused more on atomic swap protocols. They also provided future directions limited to atomic swap protocols. Monika and Bhatia surveyed blockchain interoperability solutions which have been developed for blockchains. They provided no future research directions. Belchior et al. presented a systematic literature review of blockchain interoperability. They discussed generic blockchain open issues and challenges. They mentioned some research directions based on their review. Johnson et al. presented a review on technologies enabling communication between blockchain sidechains. Future research directions were not provided here too. Schulte et al. discussed the need for blockchain interoperability and potential approaches (taken transfers and smart contract interaction) to develop interoperability solutions. The discussed some interoperability solutions based on the approaches they mentioned and provided research directions for the approaches they mentioned. Khan et al. presented a review on blockchain interoperability, whilst focusing

TABLE 1 Comparison with related works

Review Paper	Pros and cons	Target domain	Comparison	Open issues	Research directions	Heterogenous blockchains
Qasse et al.	x	✓	x	X	✓	x
Mohanty et al.	x	x	✓	✓	✓	x
Monika and Bhatia	x	x	x	✓	x	x
Belchior et al.	x	✓	✓	✓	✓	x
Johnson et al.	x	x	✓	x	x	x
Schulte et al.	x	x	x	x	✓	x
Khan et al.	x	x	✓	✓	✓	x
Velloso et al.	x	x	x	x	x	x
Talib et al.	✓	x	x	x	x	x
This paper	✓	✓	✓	✓	✓	✓

on the role of smart contracts in interoperability solutions. The discussed some challenges and presented future research directions. Velloso et al. presented a review on blockchain interoperability, focused on virtual machine migration between blockchains. Future research directions for blockchain interoperability were not discussed in their paper. Talib et al. provided a systematic review of solutions used to create interoperable blockchains. They presented future research directions mentioned in the papers they reviewed, but did not provide any research directions from their point of view.

Table 1 shows a comparison between the related literature reviews and this paper. Pros and Cons indicates if the paper discussed the advantages and disadvantages of reviewed interoperability solutions. Target domain indicates if reviewed solutions had their target domain (cryptocurrency or arbitrary data) specified. Comparison is an indicator of the authors comparing the reviewed solutions. Additionally, there is an indication of whether authors discussed open issues and future research directions. Heterogenous blockchains indicates if the authors reviewed works with a focus on heterogenous blockchains.

This paper presents a review of blockchain interoperability solutions under three major well-known categories. Advantages and disadvantages of solutions are discussed, while also comparing solutions with each other. The paper highlights the difference between digital value exchange and arbitrary data exchange and the target domain for each proposed solution. Also, the fact that other blockchain use cases do not benefit from most of the proposed interoperability solutions as they are skewed towards cryptocurrency is highlighted. Finally, possible research directions to improve upon or develop new solutions are presented.

3 | REVIEW METHODOLOGY

The paper sought to identify and provide a review of the current state of heterogenous blockchain interoperability in literature and to identify the gaps which can be filled to improve upon the development of interoperability solutions. Homogenous blockchain solutions were left out of the review because they are easier to develop since they work with the same underlying protocol and cryptographic structure. In the real world however, due to a lot of proposed blockchain architectures, many interoperability problems exist due to the different blockchain architectures being used.

Literature was collected by searching indexing databases. Databases searched include IEEE Xplore, Science Direct, Springer, Scopus and Association for Computing Machinery (ACM). These databases are known to provide a greater set of results while providing the ability to easily search and filter results. The total result obtained from the search across the considered databases was 13,462. Search strings used were "Blockchain Interoperability," "Chain interoperability," "Cross chain interoperability," "Cross chain communication," "Cross chain interfacing," "Cross chain collaboration," "Heterogenous blockchain communication," "Heterogenous blockchain interfacing," and "Heterogenous blockchain collaboration." The results obtained were further filtered by year, title, abstract and duplicates were removed. For the year, papers from January 2018 to May 2022 were considered. Titles which had no indication of solving the blockchain interoperability problem were excluded. Abstracts of the selected texts which mentioned a proposed solution to heterogenous blockchain interoperability were considered for full text reading. The results from all databases were combined and duplicates were removed. After full text reads, 14 papers from peer-reviewed literature were selected for review. These papers proposed a method for heterogenous blockchain interoperability. Table 2 shows the results of the database searches using the various search keys. The numbers in the table show the unfiltered results after the initial search. Table 3 shows the results after the various filters were applied. Table 4 shows a summary of the paper inclusion criteria. Figure 1 shows a summary of the methodology process. Additionally, some popular blockchain interoperability solutions proposed in industry were included to show the progress being

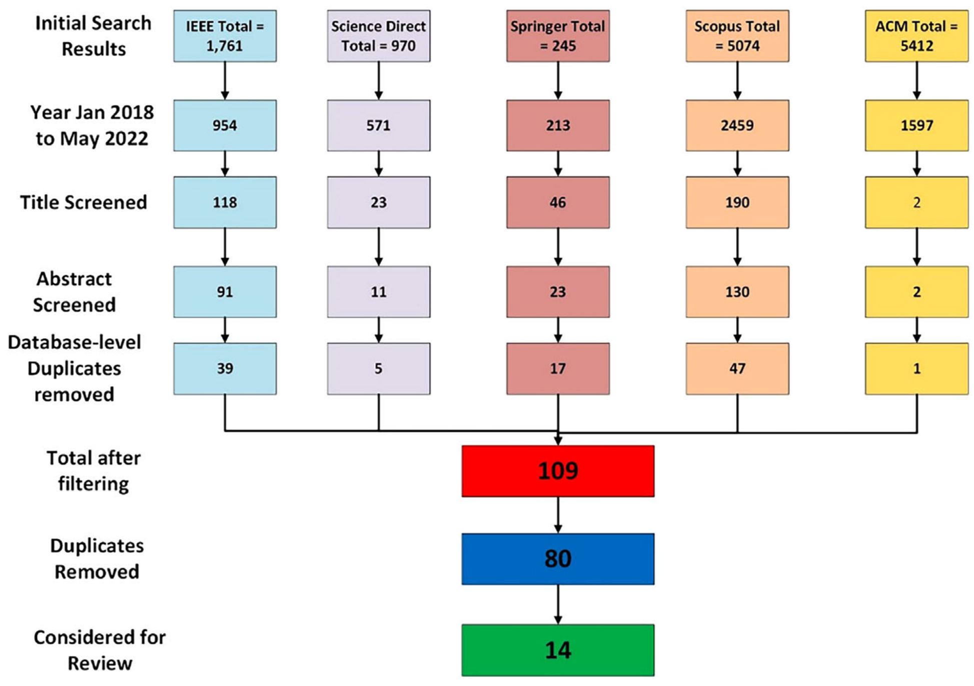

FIGURE 1 Survey methodology summary.

TABLE 2 Results of databases search

Search key	IEEE	Science Direct	Springer	Scopus	ACM
Blockchain interoperability	262	105	94	740	226
Chain interoperability	472	18	69	1790	35
Cross chain interoperability	57	18	20	182	61
Cross chain communication	561	112	35	1595	747
Cross chain interfacing	88	364	1	20	1109
Cross chain collaboration	108	101	23	683	488
Heterogenous blockchain communication	181	107	3	52	873
Heterogenous blockchain interfacing	11	77	0	0	1232
Heterogenous blockchain collaboration	21	68	0	12	641
Total	1761	970	245	5074	5412

made in both the research and industry spaces. Figure 2 shows the distribution of papers included in this survey. Other sources are web pages, articles and pre-prints.

TABLE 3 Filtered search results

Filters	IEEE	Science Direct	Springer	Scopus	ACM
Year (Jan 2018 to May 2022)	954	571	213	2459	1597
Title	118	23	46	190	2
Abstract	91	11	23	130	2
Duplicates	39	5	17	47	1
Total	109				

TABLE 4 Inclusion criteria

No.	Inclusion criteria
1	The paper proposes a solution for heterogenous blockchain communication
2	The paper presents a novel solution
3	The paper presents a clear method to solve the interoperability problem
4	The paper was published between January 2018 and May 2022

4 | STATE OF THE ART

Blockchain is a relatively new technology, and without standards to follow in developing blockchain architectures, the problem of interoperability is amplified the more. Interoperability of blockchains opens up the possibility of moving digital assets from one chain to another, making collaboration between organizations work seamlessly.

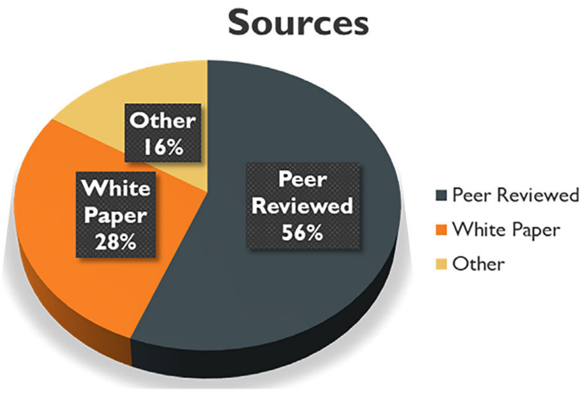

FIGURE 2 Proposed solutions distribution.

There have been different classifications of blockchain interoperability proposed in literature by different authors. Buterin [39] classified blockchain interoperability into three primary classes, namely, Notary schemes, Sidechains/Relays, and Hash locking (Hashed-Time Lock Contracts); Belchior et al. [32] classified blockchain interoperability in three major classes, namely, Public Connectors, Blockchain of Blockchains, and Hybrid Connectors, with some subcategories. Wang [2] classified them into Chain-based, bridge-based, and decentralized application-based (dApp-based), each with sub-categories. Mohanty et al. [30] also classified them under Notary Schemes, Sidechains, Blockchain Routers, Hashed Time locks, and Industrial solutions. Here, the three main interoperability directions discussed are:

1. Notary schemes
2. Hashed Time-Lock Contracts (HTLC)
3. Relays, with Relay Chains as a subcategory for Relays.

These three classes are used here as the majority of blockchain interoperability schemes tend to fall under these without overlaps. Technically, Blockchains of Blockchains, Chain based and Blockchain Routers are various names given to the concept of Relay Chains. Sidechains are used a lot in literature to describe homogenous relay-based solutions. Bridge-based interoperability could be an HTLC or a Relay, depending on the application. The three major classes are also the most widely used in literature. Figure 3 shows the classifications used by the various authors. The interoperability classes are explained in the proceeding sub-chapters, with reviews of proposed solutions presented under each class.

4.1 | Notary schemes

Notary schemes are the simplest method of realizing cross-blockchain interoperability. In notary schemes, trusted nodes agree to perform an action on a destination blockchain B when an event on a source blockchain A occurs. The concept of notary schemes is based on notarization, where a trusted witness or group of witnesses ensure execution of a contract between two or more mutually untrusted parties. The trusted nodes in this scheme are very important as any malicious action taken by them will result in a flawed interoperation process. Notary schemes are atomic; the transaction either succeeds for all parties or fails for all. A notary in this scheme is responsible for verifying the integrity and correctness of information being transferred between the blockchains. Notary schemes require no changes be made to the underlying blockchains; however, they are centralized and require the notaries to be trusted entities. The entire interoperability scheme therefore depends solely on the honesty and reputation of the notary or notaries [39].

4.1.1 | Bifröst

Bifröst is an API implementation of interoperability by Scheid et al. [40]. The proposed interoperability scheme was developed to abstract the underlying blockchains and their complexities, and allow users (developers of blockchain solutions) to easily interoperate blockchains without the need to understand the specific workings of the interoperating blockchain frameworks. Bifrost was designed to be modular, having interfaces to different blockchains to allow storage and retrieval of data on these blockchains. Bifröst was developed as part of a larger project known as the Policy-based Blockchain Agnostic Framework [41]. Bifröst has three major modules: The API, the Blockchain Adapters, and a database. The API is responsible for initiating communication with the right blockchain adapter. The adapter converts the user input into a transaction for that particular blockchain. The database keeps the credentials required for the transactions, and also stores the hash of the transaction. The remote procedure call (RPC) servers provide an isolated environment for node execution with minimal compatibility issues. Bifröst was implemented in python prototype with seven adapters for seven different blockchains and an additional PostgreSQL adapter. The authors further proposed an encryption scheme for their design to secure data moving across chains [42]. Figure 4 shows the architecture of Bifröst.

4.1.2 | Herdius

Herdius [43] works as a decentralized exchange platform aimed at providing a common linking point between all blockchains and their private keys. To make this process decentralized, one of the users' private keys is encrypted by placing the key in a hashed database, called a box, and further encrypted with another private key. This key is a Schnorr signature and is then sliced and distributed to nodes in the network. Multiple assembler nodes are capable of signing a transaction for a user by combining their pieces of the private key. For added security, none of the assembler nodes can independently decrypt the native private key completely. Instead, the transaction is signed by using homomorphic cryptography computations. Herdius

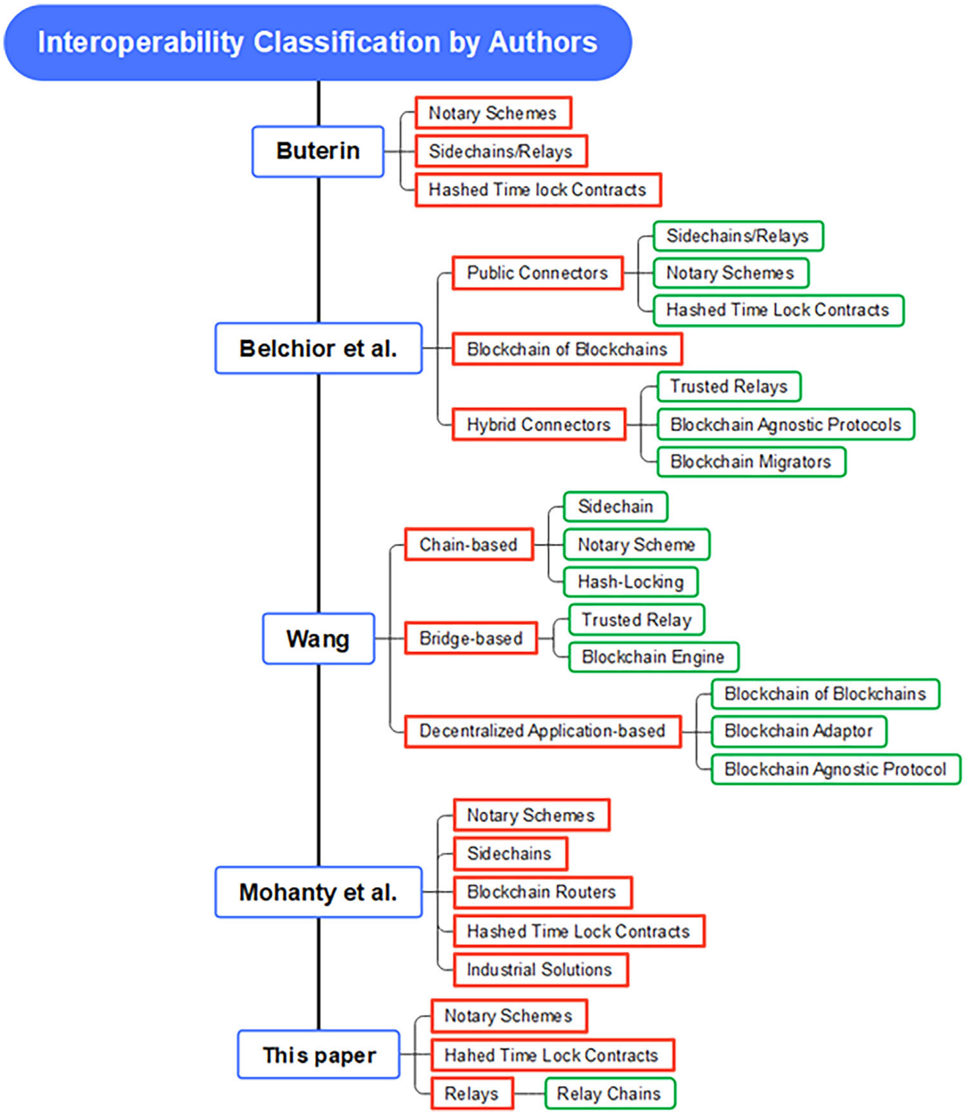

FIGURE 3 Interoperability classifications by authors.

works as an identity bridge between blockchains, allowing a user to sign transactions on one chain and have Herdius convert and transmit to another chain.

4.1.3 | Uniswap V2

Uniswap v2 [44] is an update on Uniswap v1 [45], which is a system of smart contracts residing on the Ethereum blockchain and providing a liquidity protocol which functions as a decentralized exchange. Uniswap v2 uses the same method, and supports direct swapping of cryptocurrency between Ethereum Request for Comment (ERC20) token pairs. Liquidity providers are allowed to create pair contracts for the exchanging parties. The seller of a cryptocurrency asset sends the asset to a contract created for the swap and calls the swap function. The contract completes the transaction with the second party as an atomic transaction to prevent a loss or an indefinite locking of assets. Uniswap v2 was implemented in smart contracts using Solidity smart contract language.

4.1.4 | Data migration architecture

Gao et al. [46] proposed an oracle-based cross chain data migration mechanism for heterogenous blockchains. The oracle resides between the interoperating blockchains as a trustworthy notary and is in charge of handling data migration requests and for transferring data in the migration process. The data transfer is triggered by a smart contract on receiving the user request. Asymmetric encryption is employed to ensure confidentiality and integrity during the transfer process.

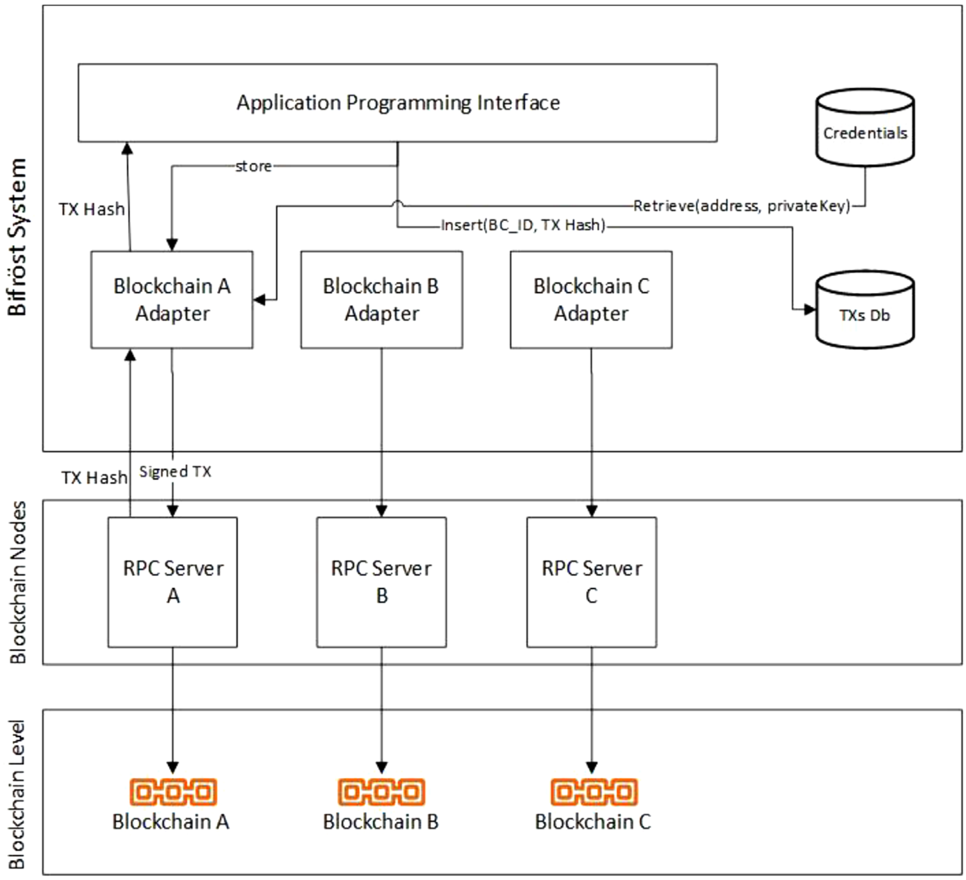

FIGURE 4 Bifröst architecture [40].

4.1.5 | Fabreum

Punathumkandi et al. [47] proposed an infrastructure for permissioned blockchain interoperability. The proposed infrastructure uses a notary to verify a blockchain event took place. A blockchain registry stores the blockchain nodes as interaction endpoints, which can be used to identify nodes for communication. A cross-chain decentralized application (CC-dAPP) linked to both blockchains is used to establish the connection between the blockchains. The Cross-Blockchain Communication Protocol (CBCP) and Cross-Chain Communication Protocol (CCCP) provide the communication rules for communication. The proposed solution was developed for interoperating Ethereum and Hyperledger Fabric.

4.2 | Hashed-time lock contracts (HTLCs)

Hash-Locking or Hashed-Time Lock contracts provide a method of exchanging value across blockchains by locking cryptocurrency assets on a blockchain X and releasing the asset after the recipient on blockchain Y confirms readiness to receive the asset. This is made possible with the technique known as atomic swapping [48, 49]. If two parties A and B residing on blockchains X and Y respectively want to exchange cryptocurrency assets, party A generates a random secret ‘s’, generates a hash ‘h’ of the secret and sends it to party B. Both parties A and B then lock their assets into a smart contract; A locking first followed by B, after B sees A's asset has been successfully locked. A then requests a claim to B's asset whilst revealing the secret ‘s’ to B. This ensures that B learns the secret ‘s’, verifies with the hash h, and claims A's asset. The entire operation is done atomically so that either the entire transaction is completed or cancelled. All transactions are also bound by time to avoid a liquidity starvation attack on any of the parties. The process is depicted in Figure 5.

4.2.1 | XCLAIM

XClaim (pronounced cross-claim) was proposed by Zamyatin et al. [50]. XClaim was developed as a generic framework to achieve trustless cross-chain exchanges using cryptocurrency-backed assets (CBA). It offers a protocol for swapping CBAs securely between existing blockchains. Blockchain-based assets are mapped one-to-one to other cryptocurrencies with the framework. Hashed Time Lock Contracts (HTLCs) are then used to complete the swapping process. The protocol uses several actors to complete the interoperation process, namely: CBA requester, CBA sender, CBA receiver, CBA redeemer,

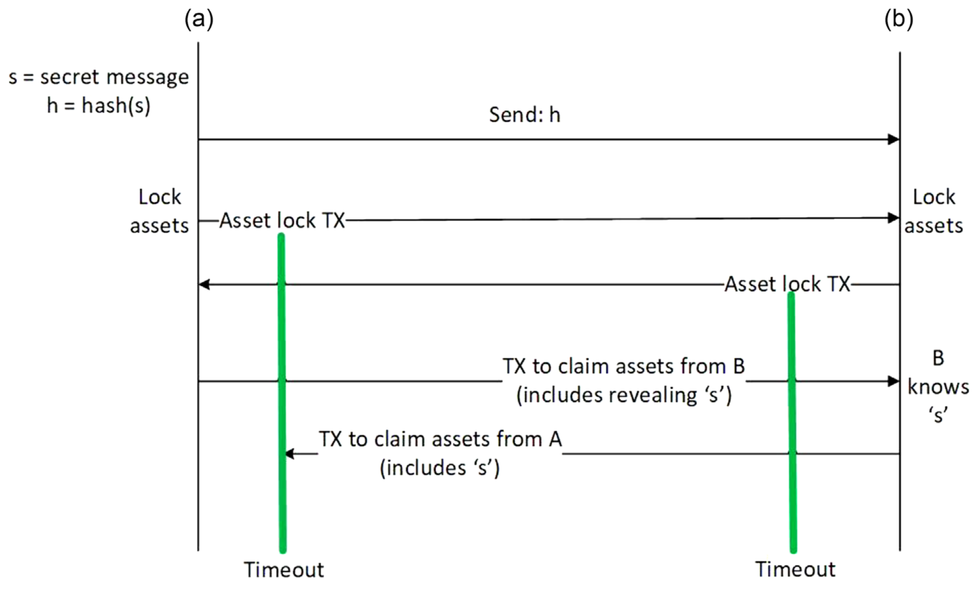

FIGURE 5 Hashed time lock contract process.

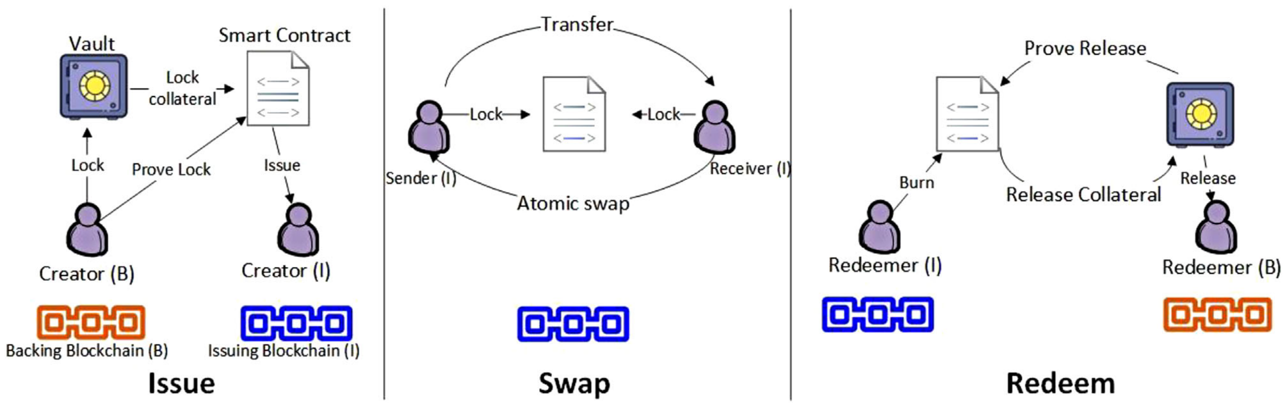

FIGURE 6 XClaim protocol execution [50].

CBA backing vault, and the issuing smart contract. A requesters locks tokens on a blockchain B before requesting an asset on blockchain I. The sender owns the asset on blockchain I and transfers ownership of the asset to the Receiver. The Redeemer then destroys the request on I and requests the corresponding amount of cryptocurrency tokens on B. The backing vault is responsible for ensuring the exchange and issuing of tokens is completed. The issuing smart contract is a publicly verifiable contract for ensuring the correct exchange of the asset on I is made. XClaim was implemented between Bitcoin and Ethereum. The architecture for the XClaim protocol is shown in Figure 6. With the issue protocol, creator (B) verifies the existence of the smart contract on blockchain I, after which funds are locked with the vault. With the swap protocol, sender (I) transfers their asset to receiver (I), with the vault being the witness to the transaction. With the redeem protocol, redeemer (I) locks their asset with the issuing smart contract, witnessed by the vault. The vault releases the locked funds to redeemer (B), after which the issuing smart contract burns the locked assets. The authors in [51] also proposed an implementation of Atomic Cross Chain Swap (ACCS) between Ethereum and Bitcoin similar to XClaim, but are yet to perform an analysis on the proposed implementation.

4.2.2 | Wanchain

WanChain [52] was developed to enable interoperability between various heterogeneous blockchains, with a focus on cryptocurrency-based blockchains. It aims at offering a platform for cross-chain operations between different blockchains. Wanchain employs multi-party computing and threshold secret-sharing technologies to achieve account management without a trusted third party. It uses a Proof of Stake (PoS) consensus algorithm to achieve between consensus between validators. Three key modules are used in the infrastructure: the

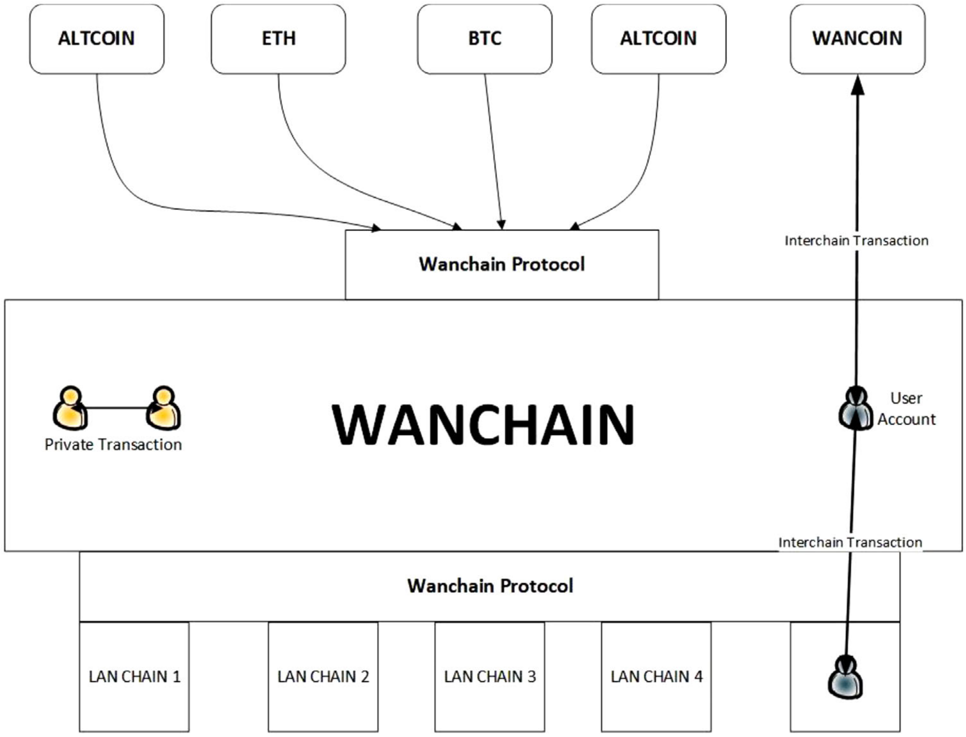

FIGURE 7 Wanchain model [52].

registration module (responsible for registering the chains and cryptocurrency assets involved in the cross-chain transaction), the cross-chain transaction data module (responsible for receiving the transaction request, acknowledging receipts of a validator returning a successful validation process or not, and ensuring the validator submits the legal transaction to the main chain) and the transaction status query module (responsible for providing query capabilities to the system). There are three categories of verification nodes: vouchers (acting as proof nodes for cross-chain transactions), storemen (acting as locked account management nodes), and validators (acting as general verification nodes). Wanchain's model is shown in Figure 7.

4.2.3 | Interledger

Interledger [53] is designed as an open protocol to enable payments across multiple payment systems. It makes it possible anyone managing accounts on two ledgers to be able to transfer cryptocurrency from one to the other. A transaction is initially proposed to a participant on the blockchain, and if accepted, both account holders authorize the transaction. The ledger then checks that funds are available for the transaction and that all rules and policies are satisfied. A ledger-provided escrow is used to enable secure payments without the need for trusted connectors. Cryptographic signatures are used by the escrow to validate the conditions for escrowing the transaction. Two modes of making transactions are possible; Atomic mode and Universal mode. The Atomic mode uses a set of notaries to ensure the entire transaction is successful, else it is aborted. A transaction commit protocol (Two-Phase Commit) is used to execute the transaction to ensure in succeeds entirely else it fails entirely. The set of notaries act as a source of truth with respect to the success or failure of the transaction. Universal mode adopts bounded execution windows and incentives to eliminate the need to use a trusted system. The incentives ensure all participants execute the transaction properly and in the right order. Interledger currently has a version 4.0 of the protocol.

4.3 | Relays and relay chains

Relay schemes provide a direct method of interoperability between blockchains. The work without trusted third parties. In these schemes, the blockchains themselves are responsible for providing information about themselves to other blockchains, and this information is verified by the receiving blockchain [35]. Block headers of blocks in the blockchain provided to the external blockchain. A block header is a compact piece of information which represents a block and contains a Merkle root of all transactions. The external blockchain first verifies the block headers using the standard block verification process of the source blockchain. The external blockchain can then verify any transaction using the provided Merkle path together with the Merkle root in the block header. Relays are generally very powerful as they can be used for asset portability, atomic swaps or any other more complex use case without restriction [35, 54]. Relay chains are relay-based schemes which employ an additional chain in the interoperability process. The central chain which enables interoperability, has validator nodes responsible for validating and executing cross-chain transactions. All interoperation requests go through this central chain which is responsible for linking the interoperating blockchains. The central chain in a relay chain solution runs its own consensus algorithm during the transaction validation phase.

4.3.1 | The inter-blockchain communication (IBC) protocol by cosmos

Initially specified by Ethan Frey [55], Christopher Goes [56] proposed a protocol for heterogenous blockchain communication. The Inter-blockchain Communication protocol was designed as a stateful protocol to enable communication between distributed ledgers. Inspired by the TCP/IP specification for network interoperability, IBC defines how different ledgers communicate using modules on each ledger. The payload data is abstracted from the IBC protocol itself, with modules determining the semantics of data packets sent and received. Modules could be independently executed pieces of logic on ledgers, for example smart contracts. IBC lies between these modules on one side and the underlying blockchain architecture on the other side. According to the authors, modules in IBC are only responsible for creating messages to be sent, with the actual relaying of messages performed by the underlying protocols for relaying messages. IBC requires the consensus mechanisms to have fast finality and does not support blockchains which have a consensus mechanism with probabilistic finality. That means Proof-of-Work-based blockchains like Bitcoin and Ethereum, two of the largest blockchain networks, are unsupported by IBC. Aside this, it requires some existing features by the host ledger including having a module system, and a key/value store. IBC protocol is used in Cosmos [57], a proposed blockchain architecture which uses a concept of zones (independent blockchains) and a hub (a central relay chain), with the hub managing transactions between zones. Tokens sent across zones are done using packets known as coin packets.

4.3.2 | Polkadot bridges

The developers of Polkadot Blockchain [27, 58, 59] proposed an interoperability solution with external blockchain networks using the concept of Bridges. The bridge is composed of two parts: the bridge relay and a bank. The bridge relay carries out consensus verification and transaction inclusion proofs of the bridged (external) chain. The bridge relay therefore understands the consensus process of the external chain. The bank is a group of actors which own bridged chain tokens on behalf of Polkadot. The bank provides a way of locking tokens or redeeming cryptocurrency cross-chain. The idea of the bridge design is based on work done in [50]. Polkadot however, has not implemented this bridge proposal, but has provided funding to interested groups willing to implement it. This has resulted in proofs of concept from Bifrost [60], Interlay [61, 62] and Chainbridge [63].

Yan Pang [64] proposed Multi-tokens Proof-of-Stake (MPoS), a consensus protocol targeting blockchain interoperability architectures. MPoS is aimed at interoperability schemes using a "Hub-parachain" architecture, mainly Cosmos and Polkadot architectures. MPoS makes it possible for staking to be done using the either the hub's native token or the parachain's token can be staked in the central hub chain. This makes it possible for more nodes to act as validators in the central hub chain to facilitate interoperability between the different blockchains.

4.3.3 | ARK ACES

Developers of the ARK [65] blockchain framework proposed ARK Contract Execution Services (ACES) [66] to enable transfers between ARK and Ethereum, Bitcoin and Litecoin. ACES uses a data section called vendor field (or SmartBridge Field), which is a 255-character field capable of allowing transactions to send text, code, instructions, hashing functions or event triggers for smart contracts. Encoded listeners, which are intermediary nodes, search through the data sent and perform the task for which the data was sent.

There is very little information on ACES and development seems to be halted currently, with links for additional documentation taken down.

4.3.4 | BTC relay

BTC Relay [67] is an implementation of smart contracts executed on Ethereum blockchain to read and verify transactions on Bitcoin blockchain. BTC Relay maintains block headers of bitcoin, creating a light version of Bitcoin blockchain on Ethereum. Relayers keep track of bitcoin block headers and submit the block headers to the BTC relay smart contract, obtaining a fee after a transaction in a block is correctly verified. This method creates a store of Bitcoin headers that can be used to verify information on Bitcoin and the presence of transactions via the stored Merkle trees. This makes verification of a transaction possible via Simplified Payment Verification (SPV). Validation of a transaction can be relayed to the deployed Ethereum smart contracts, creating several use cases, for example, the issuance of tokens.

4.3.5 | AION

The Aion Project [68] was developed to provide a multi-tiered blockchain network for interoperating multiple blockchains. It uses the hub-spoke design model, with interconnected chains interacting with a central hub chain via spokes. The AION network has four main components: Connecting Networks (which is a set of protocols for connecting the different blockchains),

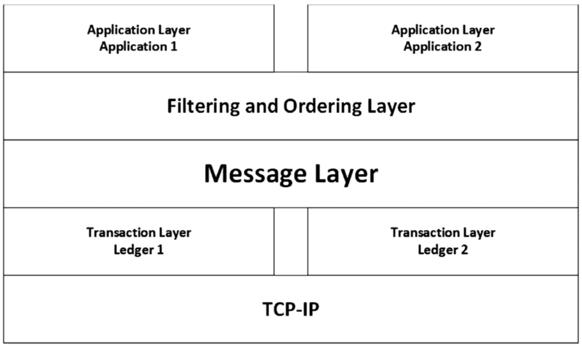

FIGURE 8 Overledger model [70].

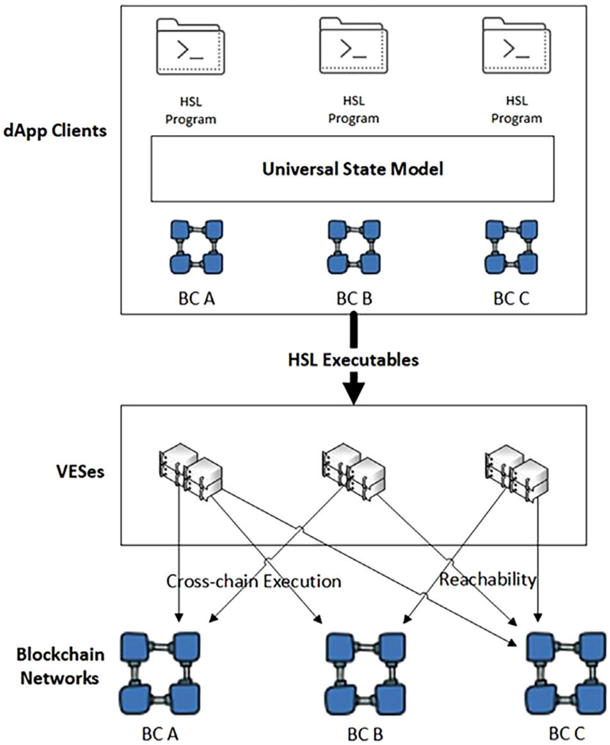

FIGURE 9 Hyperservice architecture [71].

Participating Networks (the individual blockchains), Interchain transactions, and Bridges (performing interchain transactions using a BFT-based consensus).

4.3.6 | Smart contract invocation protocol (SCIP)

SCIP [69] is a protocol proposed to provide a form of homogeneous and heterogeneous smart contract integration for smart contracts running across different smart-contract-enabled blockchains. SCIP is mainly aimed at managing smart contracts, making it possible to provide methods to trigger smart contract functions, query past events and monitor the occurrences of events. The SCIP prototype is designed to be executed at the gateway between blockchains to manage cross-blockchain transactions using smart contracts.

4.3.7 | Overledger

Overledger [70] is a proposal of a blockchain operating system capable of providing a service to allow generic applications to be executed on different blockchains. It works as an abstraction layer to abstract the underlying ledger architectures to enable interoperability at an abstracted layer, by decoupling the business logic from the ledger. The architectural design of Overledger contains four layers: A transaction layer, a filtering layer and ordering, a messaging layer, and an application layer, shown in Figure 8. The transaction layer stores transactions added to the ledger. The messaging layer retrieves and stores all the relevant information available on different ledgers. The filtering and ordering layer is responsible for relaying the various messages received from the messaging layer. The validation scheme monitors scenarios of each application and its particular specifications, and what information can be retrieved from the transaction data. The application layer is responsible for interacting with applications. Transactions are performed similar to a two-phase commit protocol scheme.

4.3.8 | HyperService

HyperService [71] is a platform and framework which provides interoperability and programmability across heterogeneous blockchain decentralized Apps (dApps). It enables dApps to be developed by providing an abstraction layer above the underlying heterogeneous blockchains, producing a unified model and a high-level language to develop dApps. HyperService uses a Universal Inter-blockchain Protocol (UIP) to manage the complex cross-chain transaction executions, which works with blockchains which have a publicly-visible transaction ledger, securely and in an atomic way. UIP is a totally trustless solution, involving no trusted third parties. HyperService has four major components: (1) dApp clients function as the connecting gateways to enable dApps connect to the HyperService platform, (2) Verifiable Execution Systems (VESes) which act as blockchain drivers, translating client-provided high-level dApp programs into transactions which are executable by the blockchain, (3) Network Status Blockchain (NSB), a blockchain of blockchains which provides an overview of the dApp execution status and (4) Insurance Smart Contracts (ISCs), responsible for guaranteeing financial atomicity in transactions. The VESes and dApp clients use the UIP protocol as their underlying infrastructure. A proposed Universal State Model describes the state transitions between the different blockchains on a virtualization layer. The architecture of Hyperservice is shown in Figure 9.

4.3.9 | SuSy

SuSy [72] is designed as a blockchain-agnostic gateway protocol for enabling cross-chain cryptocurrency asset transfer, based on Gravity [73]. Gravity was developed as a cross-chain communication between blockchains and blockchains and data oracles. Gravity nodes can decide to operate in one or more than one target chains in the Gravity network. The network uses a blockchain-agnostic oracle to enable communication between blockchains. Currently, SuSy is focused on token transferring without providing an incentive model for cross-blockchain data transfer providers. The SuSy protocol heavily depends on trusted oracles, which act as intermediaries in the asset transfer process from one blockchain to the other. The SuSy protocol is currently in the conceptual stage.

4.3.10 | Testimonium

Testimonium [74] is a blockchain interoperability proposal that depends on a validation-on-demand scheme, which uses SPV to allow on-chain verification of transactions. An incentive scheme is coupled with the validation-on-demand scheme to ensure acceptable behaviour from participants. There are two types of participants: Submitters, responsible relaying block headers from source to destination blockchain for verification and Disputers, responsible for identifying and disputing invalid block headers submitted. Testimonium works with blockchains having a data structure based on the structure proposed by Nakomoto [3].

4.3.11 | Tesseract

Tesseract [75] is a cryptocurrency exchange service which operates in real-time and uses trusted hardware to create a trusted relay for cryptocurrency asset exchange. It provides support for tokenizing secure blockchain assets which can securely map these assets to a corresponding cryptocurrency value. Tesseract enables cross-chain trading via a Trusted Execution Environment (TEE), acting as a trusted intermediary to manage funds, while keeping them safe from theft. It uses an atomic cross-chain swap protocol to ensure transactions are completely successful, else completely fail.

4.3.12 | Novel blockchain architecture for interoperability

Jin et al. [76] presented and interoperability architecture for multiple blockchains. They considered a layered approach to interoperability. Their architecture has two modes in which it can operate: an active mode and a passive mode. In the active mode, a blockchain submits a request to a second blockchain and waits for a response. In the passive mode, a blockchain monitors a second blockchain for events and transactions Their proposed cross-chain interaction model is shown in Figure 10. The layered architecture consists of data layer which unifies the format of transactions between the interoperating blockchains. The network layer enables communication between the blockchains and the consensus layer maintains consistency of the blockchain states. The contract layer maintains smart contracts to be executed cross-chain and the application layer is where the blockchain application resides.

4.3.13 | AppXchain

Madine et al. [77] proposed appXchain, a cross-chain interoperability at the application level. The proposed solution uses decentralized applications as a translation layer for multiple blockchains, using smart contracts residing on the blockchains. Verifier nodes on the network act as light clients to access data on the blockchains as well as running web services for off-chain data access and communications. The verifiers verify that information requests are valid and data moving between chains is also valid. A reputation system is used to regulate the actions of the verifier nodes. The main point of interoperability in the system is the cross-chain hub dApp (CCHDA). The CCHDA enables cross-chain communication using APIs associated with each blockchain, with a fusion interface layer integrating the communication process between the blockchains. AppXchain was implemented with blockchain-based healthcare systems as a use case. Electronic medical records were transferred between blockchains.

4.3.14 | Move protocol

Fynn et al. [78] proposed a protocol known as Move to provide operations to developers to enable the movement of contracts and objects between blockchains. The Move protocol works in two main steps; a smart contract is locked in the source blockchain in the first step and the second step reproduces the smart contract in the destination blockchain. The state of the smart contract with the data is locked in the source blockchain in the first step, effectively deactivating it and ensuring it cannot be modified at the source. Proof of the state of the smart contracted is determined at the destination chain with a Merkle proof. The smart contract is then reconstructed on the destination blockchain, where it activated for use. The two-step atomic approach was used as opposed to the popular two-phase commit (2PC) to reduce the level of coordination between the communicating blockchains. The Move protocol was implemented in modified versions of Ethereum and Hyperledger Burrow.

4.3.15 | Committee-based relay

Wu et al. [26] proposed a framework for heterogenous blockchain communication based on a periodical committee rotation scheme. The proposed system works as a relay chain with relay-chain nodes periodically replaced. The relay-chain nodes are elected from the participating blockchains to form a committee responsible for cross-chain data sharing. Information shared across blockchains is verified using Simplified Payment Verification [79].

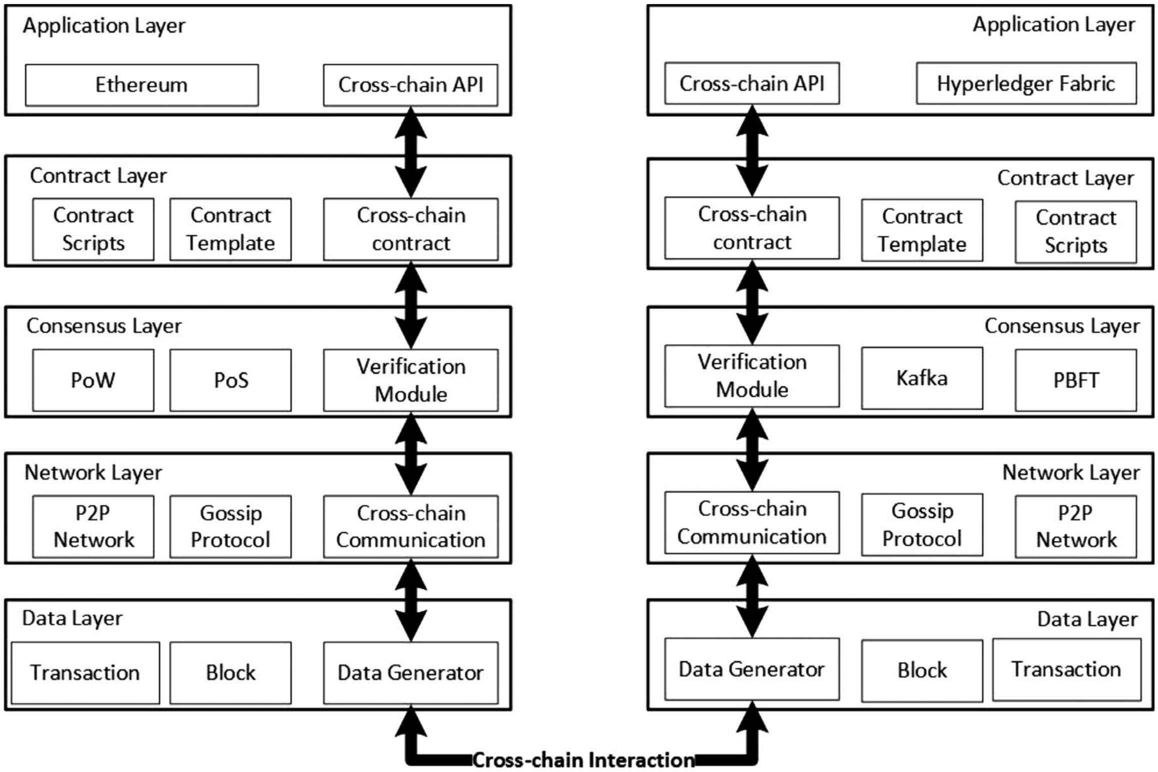

FIGURE 10 Layered cross-chain interaction model [76].

Zhou et al. [80] also proposed a similar relay-chain solution. Their solution used static nodes on the relay chain as validators and verification of the state of data was performed through a consensus process.

4.3.16 | Interactive multiple blockchain architecture

Luo et al. [81] proposed a multi-chain communication system. The system uses a router blockchain to enable message passing between multiple blockchains. The system has two main components to enable interoperability which are: Routing management, responsible for the routing messages and Crossing chain protocol, responsible for executing the cross-chain transaction. A chain joins the router network and nominates one of its nodes to become the router node. The router nodes maintaining details and routing information of all other participating blockchains in the form of a routing table. Data to be transferred from one chain to another is done using the routing information in the routing table.

4.3.17 | HERMES

Belchior et al. [82, 83] proposed a middleware for blockchain interoperability known as HERMES. HERMES is a gateway which connects two blockchains for communication. The main building block of HERMES is an extension of the Open Digital Asset Protocol (ODAP) known as ODAP-2PC. ODAP is used in the relay mode for gateway-to-gateway cryptocurrency transfers. Each gateway is aware of the other gateways either directly or through a gateway registry. The gateways are responsible for resolving identities and asset information, as well as establishing a secure channel for communication. ODAP-2PC provides fault tolerance to the system by handling gateway crashes to ensure continuous operation of the communication process.

5 | Summary

A map of the reviewed proposed solutions is shown in Figure 11. The figure shows the categorization of the various proposed solutions and includes a sub-heading for relay schemes which employ a relay chain as part of the solution. A summary of the proposed solutions is also presented in Table 5. The advantages, drawbacks and interoperability category targets are presented in the table.

6 | DISCUSSION

The blockchain interoperability problem arose due to the rapid development of the technology since it was first implemented in 2008. There have been many other proposed blockchain solutions since then but due to the lack of standards, there is no

TABLE 5 Summary of the reviewed proposed solutions

Interoperability solution	Interoperability type	Method	Advantages	Drawbacks	Target
Bifröst [40] (Peer Reviewed)	Notary	Uses a modular API to store and retrieve data on blockchains	Modular, easy to implement (no modification to blockchain frameworks), works with multiple blockchains	Introduces trust and centralization in the blockchains.	Data based
Uniswap [44] (Whitepaper)	Notary	Uses a pair of smart contracts to exchange cryptocurrency assets between traders	Relatively uncomplicated decentralized exchange service decentralized exchange service	Works only with ERC20. Security of the entire system depends largely on the security of the contracts.	Cryptocurrency
Herdius [43] (Web article)	Notary	Uses a concept of private key slicing and reassembly to transfer funds from Herdius compatible wallets to other blockchains	Multi-encryption secures transactions. No need for additional communication channels to other chains	Central chain acts as a middleman	Cryptocurrency
Data migration architecture [46] (Peer reviewed)	Notary	Employs an oracle working with a smart contract for data migration between chains	Encryption employed maintains confidentiality and integrity of data Uses a relatively simple notary mechanism in combination with a smart contract	The oracle introduces centralization Requires oracle to be trusted	Data based
Fabreum [47] (Peer reviewed)	Notary	Uses a CC-dApp, smart contracts and notaries to enable interoperability between Ethereum and Hyperledger Fabric	Blockchain nodes are stored in a registry for easy location Rules for communication are provided by the CBCP and CCCP	Works only between Ethereum and Hyperledger Fabric	Data based
Xclaim [50] (Peer reviewed)	HTLC	Uses smart contracts for cross-chain exchanges with cryptocurrency-backed assets.	Uses publicly verifiable smart contracts to eliminate trust. Requires only base ledger functionality to operate.	Consensus verification depends on the consensus used by backing blockchains	Cryptocurrency
Wanchain [52] (Whitepaper)	HTLC	Uses multi-party computing and threshold secret-sharing for cross-chain communication	Fully Decentralized. Final transaction has only one signature. No modification to original chain mechanisms.	Requires blockchains register on Wanchain to interoperate	Cryptocurrency
Interledger [53] (Whitepaper)	HTLC	Uses an ad-hoc group of notaries or a bounded execution window for cross-chain transfers	Two-phase commit ensures all systems are ready to complete the transaction. Transfers are executed atomically.	Requires the blockchain to enable escrowed transfers	Cryptocurrency

(Continues)

TABLE 5 (Continued)

Interoperability solution	Interoperability type	Method	Advantages	Drawbacks	Target
IBC [56] (Whitepaper)	Relay	Protocol for sending messages as packets from one blockchain to another. Uses an IBCBlockCommitTX to allow for proof of its most recent block-hash, and an IBCPacketTX to allow for proof of a posted transaction using a Merkle proof at the destination	Runs simultaneously between any number of ledgers connected. Payload data is abstracted from the protocol.	Only works with fast finality consensus mechanisms. Proposed for use in cryptocurrency-based blockchains Additional requirements are needed on host blockchain including key/value store and a module system for compatibility	Cryptocurrency
ARK ACES [66] (Whitepaper)	Relay	Uses a vendor field and encoded listener nodes to communicate with other blockchains over a Smart bridge	The encoded listener node allows for any other blockchain to communicate with others via the SmartBridge	Not a fully centralized solution. Requires other chain to be SmartBridge enabled.	Cryptocurrency
Polkadot bridges [59] (Whitepaper)	Relay chain	Uses a bridge containing a bridge relay and bank which carries out consensus verification and transaction inclusion proofs of the external chain.	Cross-chain transactions are submitted using a simple queuing mechanism based on a Merkle tree.	Interoperability only works between Polkadot and other chains. Relay bridge needs to understand consensus process of external chain	Cryptocurrency
BTC Relay [67] (Web page)	Relay	Uses a set of relays to submit bitcoin headers to an Ethereum smart contract to verify bitcoin transactions	It is decentralized and requires no trust between nodes	Works only one way from Bitcoin to Ethereum	Cryptocurrency
AION [68] (Web page)	Relay Chain	Uses bridges to implement a BFT-based consensus algorithm to perform cross-chain transactions	Uses a 2-phase commit protocol to ensure atomicity	Interoperating chains must be compatible with Aion	Cryptocurrency
SCIP [69] (Peer reviewed)	Relay	Provides an interface, reachable by a Smart Contract Locator which provides methods to invoke smart contract methods and monitor transactions cross-chain	Different data types are supported	Supports only two blockchains currently	Data based
Overledger [70] (Whitepaper)	Relay	Decouples the transaction layer from the messaging layer by introducing a Blockchain Programming Interface and a Verification block.	Allows simultaneous operations across multiple blockchains	The message layer can be easily overwhelmed with messages.	Data based

(Continues)

TABLE 5 (Continued)

Interoperability solution	Interoperability type	Method	Advantages	Drawbacks	Target
HyperService [71] (Peer reviewed)	Relay chain	Uses a virtualization layer on top of blockchains to enable interoperability	Blockchain agnostic. Developer facing framework included for easy integration.	Additional blockchain used for interoperation	Data based
SuSy [72] (Preprint)	Relay chain	Based on gravity and uses an intermediary oracle for cross-chain token swaps	Can be used on blockchains which support smart contracts	Trust is required of the oracle network. Cannot be used for other types of blockchain communication (data exchanges).	Cryptocurrency
Testimonium [74] (Peer reviewed)	Relay	Uses a validation-on-demand pattern to validate relayed block headers	Validations executed on chain and requires no trust.	Requires destination chain to provide scripting language to implement interoperability algorithm.	Cryptocurrency
Tesseract [75] (Peer reviewed)	Relay	Relies on a trusted execution environment to run light blockchain clients	Uses a second signature for double attestation. Executes atomic cross-chain transfers.	Relies on a trusted execution environment, making it behave like a trusted third-party	Cryptocurrency
Novel blockchain Architecture for Interoperability [76] (Peer reviewed)	Relay	Proposed interoperability architecture spanning the data, network, consensus, contract and application layers.	Provides a way to interoperate blockchains across all communication layers.	Lack of blockchain-specific standards makes solution specific to a few blockchains	Cryptocurrency
AppXchain [77] (Peer reviewed)	Relay	Uses a decentralized application as a translation layer	Blockchain agnostic. Reputation system monitors verifier nodes	Data operations are performed off-chain. Verifier nodes can access sensitive patient data during translation	Data based
Move Protocol [78] (Peer reviewed)	Relay	Uses smart contracts to move data between blockchains	Smart contracts can consistently migrate between chains	Smart contract support is required	Data based
Committee-based Relay [26] (Peer reviewed)	Relay chain	Uses a periodically rotating committee on a relay chain to enable interoperability	A message-oriented verification mechanism speeds up message verification on the relay chain	The relay chain relies on trusted nodes	Data based
Interactive multiple blockchain architecture [81] (Peer reviewed)	Relay chain	Makes use of a blockchain router to route information between connected blockchains	Transactions are atomic and consistent across chains	Router node failure prevents the interoperability process to be completed	Cryptocurrency
HERMES [82] (Peer reviewed)	Relay	Uses a middleware to enable interoperability between blockchain gateways	Interoperation operations are atomic and consistent Gateways are fault-tolerant	Gateway nodes are susceptible to DoS attacks	Cryptocurrency

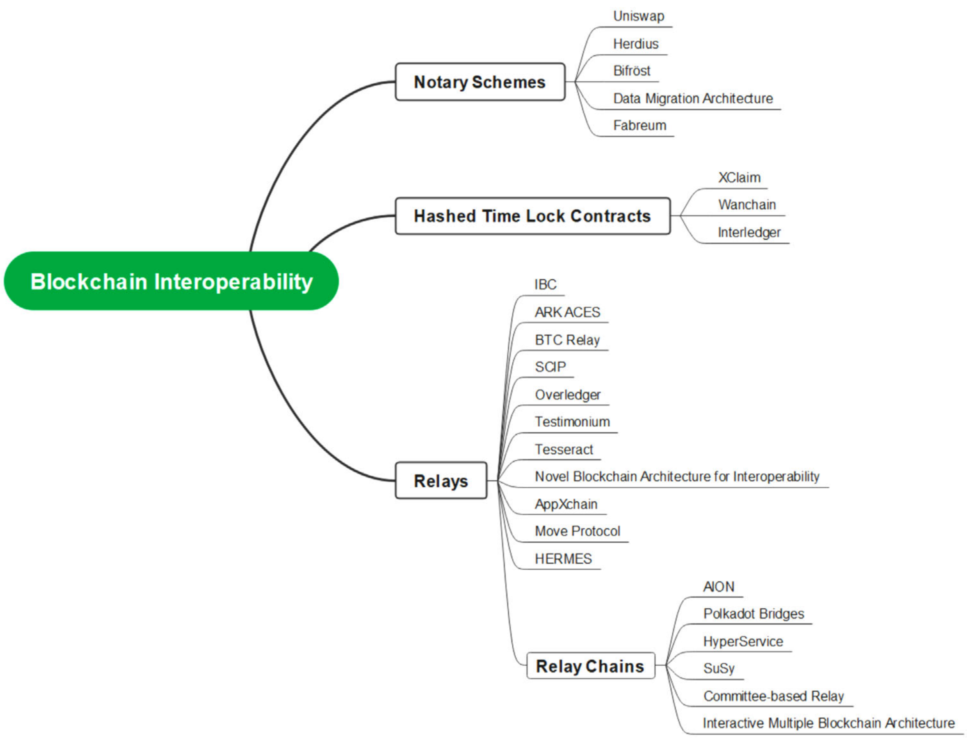

FIGURE 11 Taxonomy of the reviewed proposed solutions.

common ground for interoperation. The various interoperation solutions proposed have sought to solve this problem, but a lot more work has to be done on this topic to see real-world implementations on a substantial scale.

When looking at the proposed solutions included in this paper, it is realized that a lot of effort has been made by industry players, with the research community accounting for a little over 50% of proposed solutions, with industry players proposing 44% of solutions. This may be attributed to the fact that blockchain interoperability is still at an early stage and use cases for such solutions are still being identified. On the other hand, industry players seem to want to capitalize on the growth of the technology and its potential for the future, especially with the cryptocurrency use case. Without standards, having a way of trading currency on a platform means developers stand to earn from fees involved in making those trades. Some others like Polkadot and Cosmos, also want to be able to have their proposed blockchain solutions communicate with other more established blockchains to make it a good selling point to new blockchain adopters. There is however not a lot of information provided by industry players in their solutions, and this can make development of interoperability solutions progress at a much slower pace than if the research community was heavily involved.

Table 6 is a comparison of the reviewed solutions proposed. "Proof of concept" is an indication of whether some form of implementation or experimentation was carried out by the authors. "Fully decentralized" solutions run without any trusted third-party, central chain or group of trusted intermediaries or nodes to enable interoperability. "Existing BC frameworks unmodified" is an indication of whether the underlying blockchain frameworks involved in the interoperation action require some changes or modifications to allow the proposed solution to work, for example, addition of smart scripting capabilities. "Blockchain agnostic" solutions describe solutions which work with any set of blockchain and are not targeted towards a specific set of blockchains. Cryptocurrency-based interoperability solutions target cryptocurrency operations, whilst data-based interoperability solutions target transfer of arbitrary data [84].

A lot of effort has gone into developing interoperating schemes for cryptocurrency-based chains. This is understandable as the early implementations of blockchain were financial based. The idea behind cryptocurrency interoperability is to be able to trade with different 'coins' or exchange different 'coins' similar to fiat currency. Cryptocurrency exchange can be done using message passing. without assets moving physically between chains. The source chain updates its ledger with the exchange, sends a message to the destination chain indicating the exchange, and the destination chain also updates its ledger with the exchange. Currency-based interoperability is however difficult, if not impossible, to implement directly. The direct method of interoperability requires cryptocurrency to physically move between chains. That requires reducing tokens on one chain, and increasing tokens on another, which is near impossible unless one is a subset or sub-chain of the other. Increasing or decreasing the total tokens present on a blockchain presents additional security concerns; a malicious party could possibly

TABLE 6 Comparison of proposed solutions

	Proof of concept	Fully Decentralized	Existing BC frameworks unmodified	Blockchain agnostic	Cryptocurrency-based interoperability (Cryptocurrency)	Data-based interoperability (Information)
Bifröst	✓	x	✓	✓	✓	✓
Uniswap	✓	x	x	x	✓	x
Herdius	✓	x	x	✓	✓	x
Data migration architecture	x	x	✓	x	✓	✓
Fabreum	✓	x	✓	x	✓	✓
Xclaim	✓	x	✓	✓	✓	x
Wanchain	✓	✓	✓	x	✓	x
Interledger	x	x	✓	✓	✓	x
IBC	✓	x	x	x	✓	x
ARK ACES	✓	✓	✓	x	✓	x
Polkadot bridges	✓	x	✓	x	✓	x
BTC Relay	✓	✓	x	x	✓	x
AION	x	x	✓	x	✓	x
SCIP	✓	x	✓	x	✓	✓
Overledger	✓	x	✓	x	✓	✓
HyperService	✓	x	✓	✓	✓	✓
SuSy	x	x	✓	x	✓	x
Testimonium	✓	x	✓	x	✓	x
Tesseract	✓	x	✓	x	✓	x
Novel blockchain architecture for Interoperability	x	x	x	✓	✓	x
AppXchain	✓	✓	✓	x	✓	✓
Move protocol	✓	✓	x	x	✓	x
Committee-based relay	x	x	✓	✓	✓	✓
Interactive multiple Blockchain Architecture	x	x	✓	✓	✓	x
HERMES	x	x	✓	✓	✓	x

exploit and increase the tokens on the blockchain for their personal account [85].

Data-backed use cases of blockchain however require physically moving data from source to destination chains. Data needs to be presented on the second chain as a transaction which is appended onto the ledger, while maintaining integrity and trustworthiness of the data. These solutions a gradually being developed as the use cases keep growing.

Majority of interoperability solutions proposed so far introduce some form of centralization or trust into the system. Blockchains have decentralization as a major property. Having a solution which introduces some form of centralization into blockchains breaks the highly touted property of decentralization. Centralized solutions are easier and simpler to implement, however there are decentralized solutions being developed, albeit at a slow pace.

Relays are increasingly becoming the go-to for interoperability solutions. Relays generally offer more flexibility in interoperability while providing decentralization: a major selling point of blockchain. With relays, it is possible to transfer any form of data, unlike with HTLCs where currency trading is its only feasibility. Solutions based on notary schemes are dwindling, even though they were the first to be implemented. This is because they introduce centralization into the blockchain systems and require trust between the blockchain nodes. They are simple to develop but with the progresses being made with HTLCs and relays, focus has been shifted to enable development of solutions which are in line with the principles of blockchain.

The lack of practical, real-world implementation [31] with a number of the solutions provided is also noteworthy. Some solutions proposed over two years ago still have yet to see any form of implementation.

Blockchain use cases are increasing, and so is the need for interoperability between blockchain-based systems. Even though work is being done in this field, the research community needs to get involved on a much larger scale to speed up developments in this area.

7 | OPEN ISSUES AND POSSIBLE RESEARCH DIRECTIONS

With blockchain being implemented outside of the financial world and being seen as the 'decentralized internet,' there needs to be more focus on interoperating data-backed blockchains, which require moving of data across blockchains. This process needs to maintain the integrity, security and decentralized nature of blockchain operations while eliminating the absolute need for trust between collaborators. Also, looking at the interoperability problem with respect to data, not currency management, gives a basic starting point to working with the blockchain interoperability problem.

The gap between theory and application is an issue which has been identified. Several solutions are proposed in theory, but are yet to see a practical implementation of any sort. This may be due to the complex frameworks on which blockchains are built on, and for some of the solutions may require modifying the underlining blockchain framework.

A possible direction for research is interoperability architectures that reside above the blockchain level, but work with the blockchain to verify data. These could be application layer solution which are tightly linked to the blockchain layer to enable easy development and blockchain-agnostic interoperability schemes. Such solutions seem feasible; however, the security of the application layer needs to be strengthened to avoid application layer attacks on the blockchain.

Blockchain systems inherently suffer from the scalability issue. Most blockchains systems suffer when they need to be scaled up [86] and with cryptocurrencies, this usually translates to higher transaction fees at peak times when the number of transactions is very high.

Solution approaches could be looked at from different perspectives, for instance, Hardjono [87, 88] presents idea of blockchain gateways as presented in Figure 12, similar to how the internet operates. Taking a look at interoperability from that perspective helps to provide more possibilities in developing interoperability solutions which may be more scalable. An example could be the use of peer-to-peer networks, like in Figure 13, to provide load sharing and additional security in data movement functions, coupled with Simplified Payment Verification [89] to maintain transaction integrity. This could prove to be a fully decentralized setup which makes blockchains a truly peer to peer technology.

Connecting private blockchains to public blockchains is an area not really studied in literature. The ability to connect public and private blockchains will result in hybrid blockchains, which have a potential of further broadening the use cases for blockchains. The private-public interoperability gap is mainly due to the security requirements of these different blockchain types. Obtaining state from a permissioned chain effectively is usually the problem as a permissioned chain is built to be closed to the public.

Migrating data from a private to a public chain could be a research direction to take. The ability to share data with a public blockchain while maintaining integrity of the data and security of the permissioned chain will serve as a starting point to enable a bidirectional interoperability between the two. This is because public chains usually have no restrictions on who can submit data to be appended to the blockchain and the larger number of nodes typically means very little chance of a 51% attack and data can be verified and easily accepted or rejected by honest nodes. Successfully sharing data from a permissioned chain to a public chain will provide a foundation for also enabling data sharing from the public to permissioned chain.

The lack of blockchain standards has caused a lot of blockchains to be developed in isolation from each other. Even with technical interoperability solutions being proposed, most of the blockchains are semantically incompatible. To solve this problem, blockchain adapters can be used to convert or interpret data from one to the other without losing meaning or important data. A secure blockchain adapter will make it easy to achieve interoperability at any layer of the blockchain.

Another possible direction to further study is the use of smart contracts for interoperability [36]. Smart contracts, first proposed by Szabo [90], have provided more complex functionality to blockchains. Although smart contract implementations differ across platforms, they have similar functionality [91]. Smart contracts are written in the form of scripts which take input data and interact with the blockchain to change the state, perform authentication of a transaction and much more. With smart contracts being implemented on more blockchain solutions being proposed, this provides a promising future for having production-level blockchain interoperability based on smart contracts [92]. Some solutions have already used smart contracts in interoperability, and with smart contracts becoming a common ground for most newer blockchains, it is worth investigating additional methods to use them for interoperability.

As researchers work towards closing the gaps in blockchain interoperability, an important aspect to consider is the ability to trace data which has been moved between blockchains. This could be an area for additional research to be done as more blockchain-based traceability applications are developed. The ability to trace the path of items through data on multiple blockchains could play a major role in persuading more organizations to collaborate through blockchains.

Industry 4.0 and Industrial Internet of Things are two major emerging application domains for blockchain technology. A lot of use cases have emerged in recent years including food and drug traceability. These typically involve several collaborating players on the supply chain. As blockchain developers are looking at adopting environmentally sustainable consensus algorithms for blockchains, some research work can focus on investigating the sustainability of interoperability solutions being developed. This could prove to be a deciding factor for mass adoption in industries.

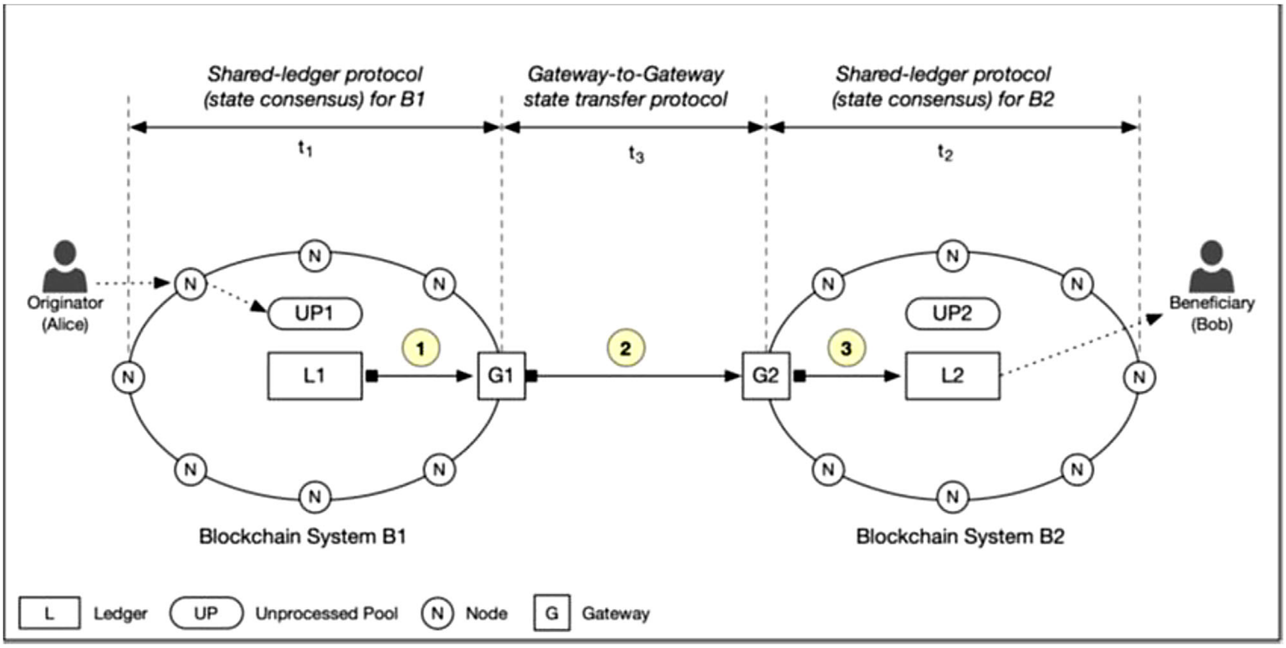

FIGURE 12 Blockchain gateways [87].

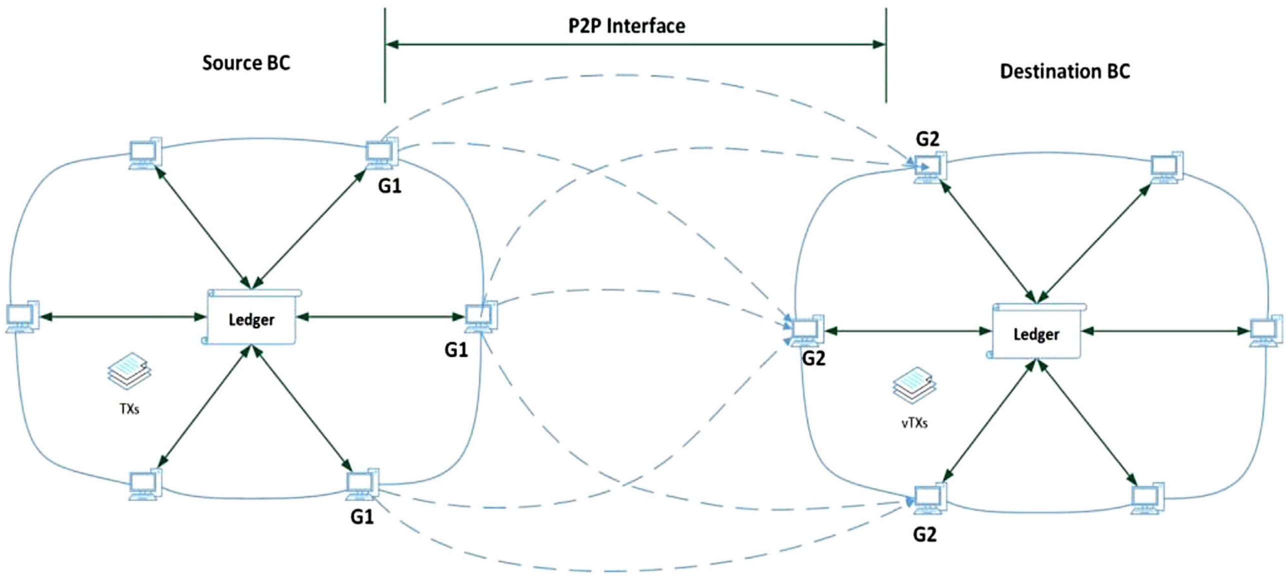

FIGURE 13 P2P Blockchain gateway.

8 | CONCLUSION

Heterogenous blockchain interoperability is becoming important problem researchers are proposing solutions to solve. This is due to the lack of blockchain-specific standards and the fact that blockchain architectures were developed in silos, without much consideration for other proposed architectures. Development of proposed interoperability solutions has seen an increase in recent years as more industries adopt blockchain.

Here, the current state of heterogenous blockchain interoperability solutions has been discussed. The solutions were compared, the blockchain application areas they target were identified their shortcomings were discussed. Some potential directions researchers can take in developing improved solutions were presented, including paying more attention to smart contracts and considering blockchain gateway solutions. It was also discovered that even though there are a number of proposed solutions in literature, most of these solutions have not been developed in real-world scenarios, with some not even having a proof-of-concept implementation. Also, majority of solutions targeted cryptocurrencies, however with an increase in adoption of blockchain by industries, there should be a lot more focus on developing interoperability solutions to cater for industry use cases.

AUTHOR CONTRIBUTIONS

Seth Kotey: Conceptualization, Formal analysis, Investigation, Methodology, Validation, Visualization, Writing—original draft; Eric Tutu Tchao: Conceptualization, Formal analysis, Funding acquisition, Methodology, Supervision, Writing—review and editing; Abdul-Rahman Ahmed: Conceptualization, Formal analysis, Investigation, Supervision, Validation, Writing—review and editing; Andrew Selasi Agbemenu: Conceptualization, Formal analysis, Methodology, Supervision, Validation, Writing—review and editing; Henry Nunoo-Mensah: Conceptualization, Formal analysis, Methodology, Supervision, Writing—review and editing; Axel Sikora: Conceptualization, Formal analysis, Funding acquisition, Project administration, Supervision, Writing—review and editing; Dominik Welte: Formal analysis, Methodology, Validation, Visualization, Writing—review and editing; Eliel Keelson: Formal analysis, Investigation, Resources, Visualization, Writing—review and editing.

ACKNOWLEDGEMENTS

This research received funding from the German Federal Ministry of Research and Education (Bundesministerium für Bildung und Forschung, BMBF) and the German Academic Exchange Service (Deutscher Akademischer Austauschdienst, DAAD). This paper was written as part of the Distributed IoT-Platforms for Safe Food Production in Education, Research and Industry (DIPPER) project, which is co-financed by the BMBF (Förderkennzeichen: 01DG21017) and DAAD (Projekt-ID: 57557211).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Seth Djanie Kotey https://orcid.org/0000-0003-2830-8288
Eric Tutu Tchao https://orcid.org/0000-0002-3242-9747
Andrew Selasi Agbemenu https://orcid.org/0000-0002-7426-3909
Henry Nunoo-Mensah https://orcid.org/0000-0002-8965-4371

REFERENCES

1. Haber, S., Stornetta, W.S.: How to Time-Stamp a Digital Document. In: Menezes, A.J., Vanstone, S.A. (eds) Advances in Cryptology-CRYPTO' 90. CRYPTO 1990. Lecture Notes in Computer Science, vol. 537, pp. 437–455, Springer, Berlin, Heidelberg (1991)
2. Wang, G.: SoK: exploring blockchains interoperability. International Association for Cryptologic Research (IACR) Cryptology ePrint, 1–27 (2021)
3. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org. 1–9 (2008). Accessed 4 October 2021
4. Fernández-Caramés, T.M., Fraga-Lamas, P.: A review on the use of blockchain for the internet of things. IEEE Access 6, 32979–33001 (2018)
5. Rauchs, M., Blandin, A., Bear, K., McKeon, S.B.: 2nd global enterprise blockchain benchmarking study. SSRN Electronic Journal. 1–72. https://ssrn.com/abstract=3461765 (2019). Accessed 19 April 2022
6. Nartey, C., Tchao, E.T., Gadze, J.D., et al.: On blockchain and IoT integration platforms: current implementation challenges and future perspectives. Wireless Commun. Mobile Comput. 2021, 1–25 (2021)
7. Alladi, T., Chamola, V., Parizi, R.M., Choo, K.K.R.: Blockchain applications for industry 4.0 and industrial IoT: a review. IEEE Access 7, 176935–176951 (2019)
8. Al-Jaroodi, J., Mohamed, N.: Blockchain in industries: a survey. IEEE Access 7, 36500–36515 (2019)
9. Teoh, B.P.C., Teoh, B.A.: Blockchain Interoperability: Connecting Supply Chains Towards Mass Adoption. In: Ismail, A., Dahalan, W.M., Öchsner, A. (eds) Design in Maritime Engineering. Advanced Structured Materials, vol. 167 Springer, Cham (2022)
10. Salimitari, M., Chatterjee, M.: A Survey on Consensus Protocols in Blockchain for IoT Networks. arXiv preprint arXiv:1809.05613 (2019)
11. Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Trans. Program. Lang. Syst. 4(3), 382–401 (1982)
12. Siegfried, N., Rosenthal, T., Benlian, A.: Blockchain and the industrial internet of things: A requirement taxonomy and systematic fit analysis. J. Enterprise Inf. Manage. 35(6), 1454–1476 (2020)
13. Ankele, R., Marksteiner, S., Nahrgang, K., Vallant, H.: Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing. In: ACM International Conference Proceeding Series. ARES '19: 14th International Conference on Availability, Reliability and Security, Canterbury CA, United Kingdom, August 26–29 (2019)
14. Thakore, R., Vaghashiya, R., Patel, C., Doshi, N.: Blockchain - based IoT: A survey. Procedia Comput. Sci. 2019, 155, 704–709
15. Abdelmaboud, A., Ahmed, A.I.A., Abaker, M., et al.: Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions. Electronics 11(4), 1–35 (2022)
16. Bhat, S.A., Huang, N.-F., Sofi, I.B., Sultan, M.: Agriculture-food supply chainmanagement based on blockchain and IoT: A narrative on enterprise blockchain interoperability. Agriculture 12(40), 1–25 (2022)
17. Lu, Q., Xu, X.: Adaptable blockchain-based systems: A case study for product traceability. IEEE Software 34(6), 21–27 (2017)
18. Phadke, A., Medrano, F.A.: A conceptual blockchain backed framework for healthcare data access – extended abstract series. Acad. Lett. 4944, 1–5 (2022)
19. Liang, X., Zhao, J., Shetty, S., et al.: Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: Proceedings of the 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'17), pp. 1–5. Montreal, QC, Canada (2017)
20. Uddin, M.A., Stranieri, A., Gondal, I., et al.: Continuous patient monitoring with a patient centric agent: A block architecture. IEEE Access 6, 32700–32726 (2018)
21. Dorri, A., Steger, M., Kanhere, S.S., et al: Blockchain: A distributed solution to automotive security and privacy. IEEE Commun. Mag. 55(12), 119–125 (2017)
22. Michelin, R.A., Dorri, A., Lunardi, R.C., et al.: SpeedyChain: A framework for decoupling data from blockchain for smart cities. arXiv:1807.01980 (2018)
23. Pillai, B., Biswas, K., Muthukkumarasamy, V.: Blockchain interoperable digital objects. Lect. Notes Comput. Sci. 11521, 80–94 (2019)
24. Zhiping, L., Dongpo, L., Bo, Z.: A cross-chain technology based on a licensed public chain. In: International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), pp. 1168–1173. Changchun, China (2022)
25. Xiong, A., Liu, G., Zhu, Q., Jing, A., Loke, S.W.: A notary group-based cross-chain mechanism. Digital Commun. Networks 8, 1059–1067 (2022)

26. Wu, Z., Xiao, Y., Zhou, E., Pei, Q., Wang, Q.: A solution to data accessibility across heterogeneous blockchains. In: Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS, pp. 414–421. Hong Kong (2020)
27. Wood, G.: An introduction to polkadot, pp. 1–17. Polkadot, Lightpaper https://polkadot.network/whitepaper/ (2020). Accessed 25 May 2021
28. Liu, Z., Xiang, Y., Shi, J., et al.: Make Web3.0 connected. IEEE Trans. Dependable Secure Comput. 5971(c), 1–15 (2021)
29. Qasse, I.A., Talib, M.A., Nasir, Q.: Inter blockchain communication: A survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track (ArabWIC 2019). Association for Computing Machinery, New York, NY, USA, Article 2, pp. 1–6 (2019)
30. Mohanty, D., Anand, D., Aljahdali, H.M., Villar, S.G.: Blockchain interoperability: Towards a sustainable payment system. Sustainability. 14(2), 1–20 (2022)
31. Monika, Bhatia, R.: Interoperability solutions for blockchain. In: Proceedings of the International Conference on Smart Technologies in Computing, Electrical and Electronics, ICSTCEE 2020, pp. 381–385. Bengaluru, India (2020)
32. Belchior, R., Vasconcelos, A., Guerreiro, S., Correia, M.: A survey on blockchain interoperability: Past, present, and future trends. ACM Comput. Surv. 54(8), 168 (2020)
33. Johnson, S., Robinson, P., Brainard, J.: Sidechains and interoperability. arXiv preprint arXiv:1903.04077 (2019)
34. Robinson, P.: Requirements for ethereum private sidechains. arXiv e-prints, arXiv, abs/1806.09834 (2018)
35. Schulte, S., Sigwart, M., Frauenthaler, P., Borkowski, M.: Towards blockchain interoperability. Lect. Notes Bus. Inf. Process. 361, 3–10 (2019)
36. Khan, S., Amin, M.B., Azar, A.T., Aslam, S.: Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability. IEEE Access 9, 116672–116691 (2021). https://doi.org/10.1109/ACCESS.2021.3106384
37. Velloso, P.B., Morales, D.C., Nguyen, M.T., Pujolle, G.: State of the art: cross chain communications. In: 2021 5th Cyber Security in Networking Conference, CSNet 2021, pp. 76–81. Abu Dhabi, United Arab Emirates (2021)
38. Talib, M.A., Abbas, S., Nasir, Q., et al.: Interoperability Among Heterogeneous Blockchains: A Systematic Literature Review. In: Rehman, M.H.u., Svetinovic, D., Salah, K., Damiani, E. (eds) Trust Models for Next-Generation Blockchain Ecosystems, EAI/Springer Innovations in Communication and Computing. 135–166 (2021)
39. Buterin, V.: Chain Interoperability, R3 Research Paper. 9, 1–25 (2016)
40. Scheid, E.J., Hegnauer, T., Rodrigues, B., Stiller, B.: Bifröst: a Modular Blockchain Interoperability API, In Proceedings of IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, pp. 332–339 (2019)
41. Scheid, E., Rodrigues, B., Stiller, B.: Toward a policy-based blockchain agnostic framework. In: 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 609–613. Arlington, VA, USA (2019)
42. Scheid, E.J., Kiechl, P., Franco, M., Rodrigues, B., Killer, C., Stiller, B.: Security and standardization of a notary-based blockchain interoperability API. In: 2021 3rd International Conference on Blockchain Computing and Applications, BCCA1, pp. 42–48. Tartu, Estonia (2021)
43. Deme, B.: What is Herdius?, https://medium.com/herdius/what-is-herdius-3831a47cfb6. Accessed 27 June 2022
44. Adams, H., Zinsmeister, N., Robinson, D.: Uniswap v2 Core, https://uniswap.org/whitepaper.pdf (2020). Accessed 30 March 2022
45. Adams, H.: Uniswap WHitepaper, https://hackmd.io/@HaydenAdams/HJ9jLsfTz🦄-Uniswap-Whitepaper (2022). Accessed 30 March 2022
46. Gao, Z., Li, H., Xiao, K., Wang, Q.: Cross-chain oracle-based data migration mechanism in heterogeneous blockchains. In: Proceedings of the International Conference on Distributed Computing Systems, pp. 1263–1268. Singapore, Singapore (2020)
47. Punathumkandi, S., Sundaram, V.M., Panneer, P.: Interoperable permissioned-blockchain with sustainable performance. Sustainability 13(20), 1–12 (2021)
48. Herlihy, M.: Atomic Cross-Chain Swaps. arXiv eprint, arXiv abs/1801.09515 (2018)
49. Miraz, M.H., Donald, D.C.: Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities. Ann. Emerg. Technol. Comput. 3(1), 42–50 (2019)
50. 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. San Francisco, CA, USA (2019)
51. Lys, L., Micoulet, A., Potop-Butucaru, M.: Atomic swapping bitcoins and ethers. In: 38th Symposium on Reliable Distributed Systems (SRDS), pp. 372–374. Lyon, France (2019)
52. Wanchain Foundation: Wanchain: Building Super Financial Markets for the New Digital Economy. White Paper Version 0.9.1, https://www.wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf, pp. 1–34 (2018). Accessed 19 February 2022
53. Thomas, S., Schwartz, E.: A Protocol for Interledger Payments. Interledger.Org. 1–25 (2015). Accessed 25 May 2021
54. Karacaoglu, Y., Mocan, S., Crown, E. A., et al.: Blockchain Interoperability, World Bank Group, Washington, D.C., vol. 1, pp. 1–62. http://documents.worldbank.org/curated/en/373781615365676101/Blockchain-Interoperability. (2018). Accessed 25 May 2021
55. Frey, E.: IBC protocol specification v0.3.1. https://ibcprotocol.org/documentation/. Accessed 20 April 2021
56. Goes, C.: The interblockchain communication protocol: an overview. https://ibcprotocol.org/documentation/ (2020). Accessed 15 May 2022
57. Kwon, J., Buchman, E.: Cosmos. https://v1.cosmos.network/resources/whitepaper. Accessed 7 June 2021
58. Wood, G.: Polkadot: Vision for a heterogeneous multi-chain framework draft 1, pp. 1–21. https://polkadot.network/whitepaper/ (2017). Accessed 25 May 2021
59. Burdges, J., Cevallos, A., Czaban, P., et al.: Overview of Polkadot and its Design Considerations. arXiv e-print, arXiv abs/2005.13456 (2020)
60. Lurpis, B.: Bifrost Finance Whitepaper, pp. 1–37. https://github.com/bifrost-finance/bifrost-wiki/blob/master/bifrost-finance-whitepaper-en.pdf (2021). Accessed 17 February 2022
61. Interlay: Interlay and Kintsugi Documentation. https://docs.interlay.io/#/. Accessed 6 June 2022
62. Zamyatin, A.: The Future of Interoperability Interlay's Vision: Trustless and Decentralized Cross-Chain DeFi. https://medium.com/interlay/the-future-of-bridging-assets-837998115f6b (2021). Accessed 3 March 2022
63. Chainbridge: Chainbridge, https://chainbridge.chainsafe.io/. Accessed 22 February 2022
64. Pang, Y.: A new consensus protocol for blockchain interoperability architecture. IEEE Access 8, 153719–153730 (2020)
65. ARK Ecosystem SCIC: ARK, pp. 1–50. https://arkscic.com/whitepaper.pdf (2019). Accessed 27 May 2021
66. Walker, T.: ACES: ARK Contract Execution Services, https://ark.io/blog/aces-ark-contract-execution-services-d6924486b8c5. Accessed 25 May 2022
67. Ethereum, Consensys: BTC RELAY. http://btcrelay.org/. Accessed 3 February 2022
68. Nuco Networks: AION, https://aion.theoan.com/. Accessed 20 April 2022
69. Falazi, G., Breitenbücher, U., Daniel, F., Lamparelli, A., Leymann, F., Yussupov, V.: Smart contract invocation protocol (SCIP): A protocol for the uniform integration of heterogeneous blockchain smart contracts BT. In: Dustdar, S., Yu, E., Salinesi, C., Rieu, D., Pant, V. (eds.) Advanced Information Systems Engineering, pp. 134–149. Springer International Publishing, Cham (2020)
70. Verdian, G., Tasca, P., Paterson, C., Mondelli, G.: Quant Overledger Whitepaper, https://uploads-ssl.webflow.com/6006946fee85fda61f666256/60211c93f1cc59419c779c42_Quant_Overledger_Whitepaper_Sep_2019.pdf (2018). Accessed 17 March 2022
71. Liu, Z., Xiang, Y., Shi, J., et al.: Hyperservice: interoperability and programmability across heterogeneous blockchains. In: Proceedings of the ACM Conference on Computer and Communications Security. CCS '19: 2019 ACM SIGSAC Conference on Computer and

Communications Security, London, United Kingdom, November 11–15, 2019, pp. 549–566 (2019)
72. Pupyshev, A., Dzhafarov, E., Sapranidi, I., Kardanov, I., Khalilov, S., Laureyssens, S.: SuSy: A blockchain-agnostic cross-chain asset transfer gateway protocol based on Gravity. arXiv e-print, arXiv abs/2008.13515 (2020)
73. Pupyshev, A., Gubanov, D., Dzhafarov, E., et al.: Gravity: a blockchain agnostic cross-chain communication and data oracles protocol. arXiv e-print, arXiv abs/2007.00966 (2020)
74. Frauenthaler, P., Sigwart, M., Spanring, C., Schulte, S.: Testimonium: A Cost-Efficient Blockchain Relay. arXiv eprint, arXiv abs/2002.12837 (2020)
75. Bentov, I., Ji, Y., Zhang, F., Breidenbach, L., Daian, P., Juels, A.: Tesseract: Real-time cryptocurrency exchange using trusted hardware. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (Association for Computing Machinery, pp. 1521–1538. London United Kingdom (2019)
76. Jin, H., Dai, X., Xiao, J.: Towards a novel architecture for enabling interoperability amongst multiple blockchains. In Proceedings of the IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, pp. 1203–1211 (2018)
77. Madine, M., Salah, K., Jayaraman, R., Al-Hammadi, Y., Arshad, J., Yaqoob, I.: AppxChain: application-level interoperability for blockchain networks. IEEE Access 9(April), 87777–87791 (2021)
78. Fynn, E., Bessani, A., Pedone, F.: Smart contracts on the move. In: Proceedings of the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2020, pp. 233–244. Valencia, Spain (2020)
79. Wright, C.S.: Merkle Trees and SPV, https://craigwright.net/blog/bitcoin-blockchain-tech/merkle-trees-and-spv/. Accessed 10 February 2022
80. Zhou, Q., Lee, Y.: A study on blockchain interoperability mechanism. J. Syst. Manage. Sci. 11(4), 127–145 (2021)
81. Kan, L., Wei, Y., Hafiz Muhammad, A., Siyuan, W., Linchao, G., Kai, H.: A multiple blockchains architecture on inter-blockchain communication. In: Proceedings - 2018 IEEE 18th International Conference on Software Quality, Reliability, and Security Companion, QRS-C 2018, pp. 139–145. Lisbon, Portugal (2018)
82. Belchior, R., Vasconcelos, A., Correia, M., Hardjono, T.: HERMES: fault-tolerant middleware for blockchain interoperability. Future Gener. Comput. Syst. 129, 236–251 (2022)
83. Belchior, R., Vasconcelos, A., Correia, M., Hardjono, T.: Enabling cross-jurisdiction digital asset transfer. In: Proceedings - 2021 IEEE International Conference on Services Computing, SCC 2021, pp. 431–436. Chicago, IL, USA (2021)
84. Hewett, N., Lehmacher, W., Wang, Y.: Inclusive deployment of blockchain for supply chains: Part 6 – A framework for blockchain Interoperability. World Economic Forum. https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-1-introduction/ (2019). Accessed 21 May 2021
85. TIWARI, A.: Wormhole hack illustrates danger of DeFi cross-chain bridges, https://cointelegraph.com/news/wormhole-hack-illustrates-danger-of-defi-cross-chain-bridges. Accessed 27 March 2022
86. Biswas, S., Sharif, K., Li, F., Nour, B., Wang, Y.: A scalable blockchain framework for secure transactions in IoT. IEEE IoT J. 6(3), 4650–4659 (2019)
87. Hardjono, T.: Blockchain gateways, bridges and delegated hash-locks. arXiv eprint, arXiv abs/2102.03933 (2021)
88. Hardjono, T., Lipton, A., Pentland, A.: Towards a design philosophy for interoperable blockchain systems. arXiv eprint, arXiv abs/1805.05934 (2018)
89. Wright, C.S.: On Merkle Trees. https://craigwright.net/wp-content/uploads/2019/11/On-Merkle-Trees_CSW.pdf, 1–5 (2019). Accessed 17 December 2021
90. Szabo, N.: Formalizing and Securing Relationships on Public Networks. First Monday. 2(9) https://journals.uic.edu/ojs/index.php/fm/article/download/548/469 (1997)
91. Bandara, E., Tosh, D., Foytik, P., Shetty, S., Ranasinghe, N., De Zoysa, K.: Tikiri—Towards a lightweight blockchain for IoT. Future Gener. Comput. Syst. 119, 154–165 (2021)
92. Nissl, M., Sallinger, E., Schulte, S., Borkowski, M.: Towards cross-blockchain smart contracts. In: International Conference on Decentralized Applications and Infrastructures (DAPPS), IEEE, pp. 85–94. United Kingdom (2021). https://doi.org/10.1109/DAPPS52256.2021.00006

How to cite this article: Kotey, S.D., Tchao, E.T., Ahmed, A.-R., Agbemenu, A.S., Nunoo-Mensah, H., Sikora, A., Welte, D., Keelson, E.: Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. IET Commun. 17, 891–914 (2023). https://doi.org/10.1049/cmu2.12594