A Brief History of Blockchain Interoperability

RAFAEL BELCHIOR, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal, Massachusetts Institute of Technology, United States, and Blockdaemon, Portugal
JAN SÜSSENGUTH, Blockdaemon, Germany
QI FENG, Blockdaemon, United States
THOMAS HARDJONO, Massachusetts Institute of Technology, United States
ANDRÉ VASCONCELOS, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal
MIGUEL CORREIA, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Portugal

Blockchain interoperability conflates the need for *distributed systems* to communicate with third-party systems without a canonical chain or orchestration layer. As there is no "chain to rule them all" (for performance, privacy, and market forces), these distributed systems rely on exchanging data and value across network boundaries. Interconnected systems achieve a higher value than the sum of their parts, similar to how the Internet emerged as a set of isolated *Local Area Networks* (LANs) - and, by force of surprising synergies, such networks fundamentally transformed society forever. Concurrently, in the last decade, we have witnessed the astonishing development of blockchain technologies, which seem more connected than ever: via *bridges* [12, 14, 15, 30], *oracles* [44], and other *interoperability mechanisms* [4, 9, 16, 47, 89]. These recent developments have, slowly but steadily, contributed to the improvement of the scalability of blockchain networks, as well as providing new functionality and use cases [66], but there is still a long way to go until mass adoption. In this paper, we will dive into the rabbit hole of blockchain interoperability and explain why it is needed, what has been done in the last decade, and where it is going.

1 EVOLUTION OF BLOCKCHAIN

The world is rapidly changing. The current socio-economic environment, including rapid digitization of information and processes, the rise of machine learning, and the ubiquitous access to the Internet [61] amplifies the need for human-human and human-machine interactions without a single point of failure that are *transparent, dependable, resilient*, and that operate at a global scale. This might ring a bell - the concept of *distributed ledger technologies* (DLT), or blockchain, refers to systems implementing these properties. More specifically, DLT refers to a distributed system of peer nodes that agree on a ledger of records; or to a data structure that implements such a ledger. The innovation that blockchain provides is the ability, for the first time in history, to convey (business) transactions in a decentralized way, allowing the existence of decentralized applications (*dApps*). Many use cases have been either developed as proofs-of-concept or deployed to production, for instance, in healthcare, supply-chain, metaverse, justice, arts/non-fungible tokens (NFTs), decentralized finance (DeFi), and many others [73]. Such systems provide *safety* and *liveness*

Authors' addresses: Rafael Belchior, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Rua Alves Redol, 9, Lisboa, Portugal, 1000-029 and Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, United States, MA 02139 and Blockdaemon, , Lisbon, Portugal, 60327; Jan Süßenguth, Blockdaemon, c/o TechQuartier, Platz der Einheit 2, Frankfurt am Main, Germany, 60327; Qi Feng, Blockdaemon, , Los Angeles, United States, 90232; Thomas Hardjono, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, United States, MA 02139; André Vasconcelos, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Rua Alves Redol, 9, Lisboa, Portugal, 1000-029; Miguel Correia, INESC-ID, Instituto Superior Técnico, Universidade de Lisboa, Rua Alves Redol, 9, Lisboa, Portugal, 1000-029.

XXXX-XXXX/2023/-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

[2], which in the distributed system research area jargon means that such systems do not allow bad behavior from participants (*bad things do not happen*), and desired behavior eventually is processed by the system (*good things happen*) [29]. How these properties are realized depends on the desirable decentralization level, the fundamental property of blockchains, and the implementation specifics.

Blockchains have been around since 2008 and come in very different flavors: from the primer blockchain and cryptocurrency *Bitcoin* [64], a system that revolutionized decentralized peer-to-peer payments without a trusted authority, to *Hyperledger Fabric*, a private blockchain framework that prioritizes privacy and scalability over decentralization [3], suitable for enterprise-grade use cases. In Bitcoin, safety (i.e., "security") is realized by the common prefix and chain quality properties [40], meaning that, at a high level, honest nodes share a common history of blocks; and that the ratio of blocks proposed by malicious nodes is upper-bounded by the ratio of blocks proposed by honest nodes. In Fabric, safety is weaker and realized in terms of accountability [45]. Accountability means that a malicious party can halt the blockchain, but it will be identifiable and, therefore punishable - a sensitive trade-off made in a business network where parties are identified and operate under a certain legal framework. Thus, it is clear that blockchains have evolved in very different directions [91].

The blockchain trilemma (cf. Figure 1), postulated by one of Ethereum's founders [19], states that blockchains have an inherent trade-off between security, scalability, and decentralization. Being an equivalent of the CAP theorem[1] for blockchains, the core property chosen is typically security - implemented through consensus algorithms, crypto-economics, formal modeling, and results from distributed systems research (namely crash-fault tolerant and byzantine-fault tolerant algorithms [29, 90]). Typically, the more nodes involved in a peer-to-peer network, the harder it is to corrupt it, but the slower the consensus becomes (intuitively, more nodes, more messages exchanged and therefore, the higher the overall communication latency). Consequently, decentralization and security walk *manus in manu.* Nonetheless, we still have to solve the scalability part of the trilemma. But how? The answer lies within the research area of interoperability, and it will be later apparent to the reader why.

1.1 The Origins of Interoperability

Wegner, a computer scientist that worked in the area of interoperability, stated that "interoperability is the ability of two or more software components to cooperate despite differences in language, interface, and execution platform" [81]. Counting with a large corpus of research [48], interoperability has been studied since the 80s [57], when engineers started observing the rise of complex software systems that communicated with other networks and systems, heterogeneous in nature. Indeed, interoperability tends to appear in a later stage of maturation of a given technology when sufficient complexity of systems requires it. In particular, this research area started gaining more notoriety with the emergence of the Internet [46]. The latter was created in a geo-political context (namely the Cold War) that required the creation of a resilient, dependable, scalable, manageable, and self-healing network that could sustain attacks from a powerful adversary. Effectively, the Internet architecture specified the number of properties that propelled it as a commercial success, enabling considerable economic growth [60]. Those properties are *survivability*, *diversity of services*, and *diversity of networks.*

Non-surprisingly, these principles anchored in the Internet architecture are guiding the development of interoperability protocols and standards, with direct application to blockchains [11, 46]. Given the history of the development of the Internet and computer networks in general, it does not come as a surprise that communities are pushing toward cross-chain interoperability. As a

[1] The CAP theorem [43] states a trade-off between consistency, availability, and partition tolerance in distributed systems.

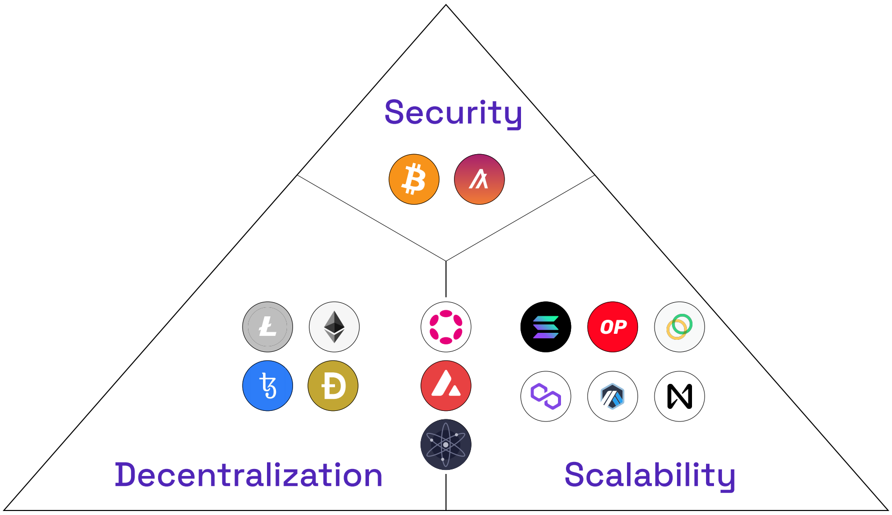


Fig. 1. Classification of blockchains according to the blockchain trilemma. We position solutions in one of three buckets (only the bucket matters, and not the relative position of a blockchain to another within the bucket). Blockchain ecosystems, left to right, up to bottom: Bitcoin, Algorand, Litecoin, Ethereum, Polkadot, Solana, Optimism, Celo, Tezos, Dogecoin, Avalanche, Polygon, Arbitrum, NEAR, Cosmos.

consequence, the world is settling on several multi-chain blockchains connected by cross-chain solutions (typically bridges, considered major players in DeFi ecosystems).

1.2 Transactions Across Distributed Ledgers

To realize transactions across distributed ledgers, we envision a distributed ledger system as an abstract representation of a distributed database. In this design, multiple replicas maintain a global state using a consensus algorithm. The global state is changed via user-submitted transactions, similar to conventional databases. Changing the state is subject to transactions adhering to specific consistency rules. Consistency rules are enforced in each database (i.e., blockchain) locally, but, additionally, have more restrictions (i.e., consistency rules) coming from the cross-chain logic [10].

In practice, these consistency rules are restrictions in a sequence of read and write operations, orchestrated across different chains. However, unlike traditional databases, a distributed shared ledger lacks a singular or unitary entity that can be relied upon for reading from or writing to it. Instead, the internal consensus protocol assumes the responsibility of ensuring safety and liveness. Typically, cross-chain transactions [49] respect a set of properties equivalent to ACID [11, 79]. Different techniques to provide ACID-like properties to cross-chain transactions enforce the correctness of cross-chain protocols, namely that cross-chain transactions are atomic: either all the local transactions are executed correctly and committed to the underlying ledger, or none are. The underlying technical challenge is *how to ensure that two or more distributed ledgers mutually agree on a specific ledger state within a defined time limit, unidirectionally or bidirectionally?*. The more researchers worked on this problem, the clearer the solutions: proving state with cryptographic proofs [12], the usage of timelocks [34], the use of state-locking [11]. And so, bit by bit, the blockchain trilemma becomes not so much of a trilemma and more like a set of tradeoffs that can preserve all three properties on different levels. And the interoperability research area continues to contribute to this trilemma because scalability *is* realized through interoperability.

1.3 Interoperability as a Requirement of Scalability of Service

Studying interoperability is a sensitive vehicle to off-load computation in a way that does not sacrifice decentralization and achieves a more balanced trade-off set in the referred trilemma. On the one hand, interoperability is a requirement for scalability. On the other, it enables more functionality.

We have two types of blockchain interoperability: *multi-chain interoperability*, and *cross-chain interoperability*. In multi-chain interoperability, instances of a *blockchain engine* [12] (aka *blockchain of blockchains*, e.g., Cosmos, Polkadot, Avalanche) communicate with each other through a trust anchor that is implemented in the protocol. Each instance of the blockchain engine (let's call them mini-blockchains) has a built-in interoperability protocol and data format that other mini-blockchains understand. Consider Polkadot's parachains: each parachain (mini-blockchain) communicates with other parachains via XCMP, a built-in interoperability format [83]. Communications are anchored by the canonical blockchain (the relay chain in Polkadot) and establish trust from one parachain to the world. In Cosmos, mini-blockchains are called zones, which communicate via a protocol called Inter Blockchain Communication (IBC) [55]. What anchors the multi-chain communication is a light-client interoperability mechanism that processes cryptographic proofs [9]. Other blockchains that claim to have incredible scalability typically use a sharding system [80], where each shard (mini-blockchain) is responsible for computing a subset of the overall transactions. The result is then communicated across-shards. However, there is a problem. Polkadot's parachains can communicate with each other, but can they communicate with Cosmos or other blockchain engines? Not natively, because they follow a different protocol and have a different global state (i.e., are *heterogeneous*). Those are the boundaries of a blockchain network (otherwise, they would be considered the same system, i.e., *homogeneous*). That is, the cross-chain vision connects heterogeneous chains; in the multi-chain vision, a native cross-chain protocol connects homogeneous chains that utilize the same framework and typically are anchored in a common chain.

To connect blockchains, we need to use cross-chain communication, a set of techniques allowing us to share data and transfer assets between blockchains [12]. This concept seems prone to security vulnerabilities, and it is indeed - more than \$2.5B in losses happened only in blockchain bridges, the most popular cross-chain applications [10, 59] (there are more than 110 bridges[2]), conquering the rank of having the most devastating attacks in terms of capital lost within DeFi applications. In part due to this, it has been pointed out by reputable people in the blockchain community that multi-chain is inherently more secure than cross-chain [18]. While the authors tend to agree that multi-chain does seem to lower the attack vector for interoperable applications, it is also the case that there will not be a blockchain to rule them all: design decisions need to be made, and some give priority to scalability while sacrificing decentralization (namely permissioned blockchains), while others focus on privacy [3], while others are even application-specific [55, 83].

Interoperability across blockchains allows the free flow of capital across ecosystems, preventing lock-in and increasing economic equality between users. It further increases synergies between blockchain communities by eliminating data and value silos (e.g., synergies at the application level[9]), while eliminating expensive duplication of data (for example, by replicating the part of the state of a blockchain on another [82]) and allowing new use cases (e.g., token holders in one blockchain to vote on decentralized autonomous organizations (DAOs) on another blockchain [38]). A bit paradoxically, it allows increasing the security of a chain by having a weaker-security blockchain to peg its state to a more secure chain (for example, sidechains [7, 74], rollups [78], or timestamping mechanisms [76]) to create periodical checkpoints on a more expensive, secure blockchain. As an example, blockchain rollups are sidechains that allow off-loading transactions

[2] https://chainspot.io/

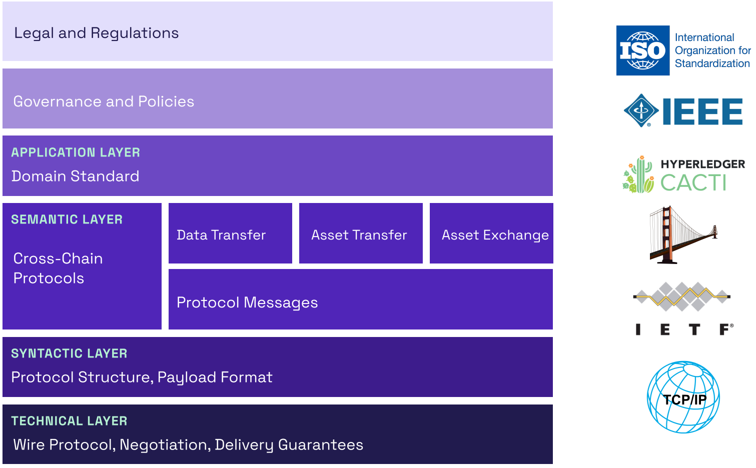


Fig. 2. Blockchain interoperability layers [9]

from a source chain to a third-party chain, and tokens to operate such a sidechain need to be bridged from the source chain [78]. Thus, we believe cross-chain interoperability is necessary, a fact supported by the extensive academic work done in the last decade [12], and the industry [25, 77], with several sources even referring interoperability as key to mass adoption [12, 26, 69].

1.4 Interoperability Layers

It is worth noting that these solutions can be partitioned into different layers [9]. The technical layer focuses on data formats, communication protocols, interface specifications, and integration services ("bits and bytes"). It precedes the syntactic layer that defines protocol structure and payload formats. Semantic interoperability exists when systems can interpret exchanged information following a defined ontology. This translates into systems being able to exchange information and assets. Several different applications can be built on top of the semantic layer (e.g., bridges on top of asset transfer protocols and functionalities).

Organizational interoperability is the set of agreements to integrate different systems realizing a use case - governance and policies (typically requires consensus from business partners or the community). Legal interoperability assures organizations can cooperate under heterogeneous legal frameworks, policies, and strategies (legal and regulations). Figure 2 summarizes the existing standardization attempts across the different interoperability layers. Having clear interfaces between the different layers both limits development complexity and provides a separation of concerns that empowers developers to think more abstractly about the underlying layers and focus on application logic. Most solutions presented in this article refer to the semantic layer. Different standards are being built for each layer. For instance, at the IETF, the Secure Asset Transfer Protocol working group [47] defines a protocol for digital asset transfers that spawns across the semantic and organizational interoperability layers.

2 DECONSTRUCTING INTEROPERABILITY - THE PRESENT

There are different types of interoperability modes acting on the semantic layer. First, the *data transfer* interoperability mode allows arbitrary data transfer to realize general cross-chain business logic [9]. Industry solutions allowing this are called *general message passing* (GMP). Hyperledger

Cacti [63] is an example of a cross-chain solution supporting this mode: it connects private to public blockchains and facilitates integration with centralized systems. Such platforms can use as building blocks multi-chain APIs such as Blockdaemon's Universal API [17].

The second type are *asset transfer* solutions, typically implemented through cross-chain bridges. In bridges, an asset is locked in an origin blockchain, and the representation of that asset is created (minted) on a target blockchain (called wrapped or synthetic assets). Bridges have been attacked consistently because the attack surface is very large [93] (malfunctioning on the different components of a bridge such as a relayer, protocol vulnerabilities, implementation bugs, network-layer attacks, and incentive mechanisms attacks).

Finally, *asset exchanges* consist in two pairs of transactions, a pair in each blockchain such that: 1) Alice transfers tokens of cryptocurrency A to Bob on blockchain 1; and 2) Bob transfers tokens of cryptocurrency B to Alice on blockchain 2. The idea is as follows: first, Alice initiates the protocol by generating a secret (a key) that will be included in a smart contract on blockchain 1. That smart contract has logic to send Bob the A tokens upon providing the secret Alice generated. Bob does the same: he deploys a similar contract on blockchain B, with a transaction sending B tokens to Alice upon providing the secret Alice generated. Alice can then redeem her tokens by providing the secret to Bob. Bob can then learn the secret and redeem his tokens on the other blockchain. Should the secret not be revealed, the smart contract expires, and assets will be redeemable by their owners. We call the procedure above an HTLC (hash time-locked contract), and different variations exist [67]. As each pair of transactions is atomic and uses native assets, this solution category tends to be safer than bridges, albeit more expensive.

2.1 A Look at the Industry

In this section, we provide an overview of industry solutions, focusing on generic messaging protocols. After that, we present current obstacles and challenges that are solved, partially solved, or still unsolved (versus 2021, when they were identified).

To understand the current interoperability landscape, note that the market has over 100 solutions today [20]. Out of these, low-level interoperability protocols are more expressive and general than the asset-specific, chain-specific, or application-specific bridges further up the stack [13], which specialize in one task. However, some of the protocols do not come with consumer-facing applications or user interfaces, and instead only provide the technical building blocks needed by external products to enable cross-chain communication, like smart contracts and low-level APIs [50]. This leads to a bad user experience and obstacles in utilization for non-expert users. Nonetheless, these technologies are evolving. Our hypothesis is that teams increasingly focus on GMP protocols [6, 36, 72] because the expressiveness of the data they can handle allows for the development of a multitude of solutions. Those solutions account for a wide range of use cases, covering all previously mentioned categories as well as bridges than can relay arbitrary messages, *arbitrary message bridges* (AMBs). One can design a GMP protocol that relays messages across blockchains, and expose APIs (on the smart contracts) that can be consumed by coordination protocols (e.g., bridges), as Figure 3 illustrates.

While compared to more limited solutions the development of generalized messaging protocols is more laborious, their creators can achieve reduced reliance on individual blockchain networks, applications, and assets. At the same time, they collect the benefits from both the utilization of their own and the products built based on their system by partners and customers, e.g., through licensing or a pro-rata share of fees.

Some examples: Axelar's Satellite, recently extended with cross-chain swaps between the protocol's synthetic and a lot of chains' native assets thanks to the implementation of third-party Squid Router; liquidity network Stargate and Aptos Bridge, both built on top of LayerZero (LZ) as

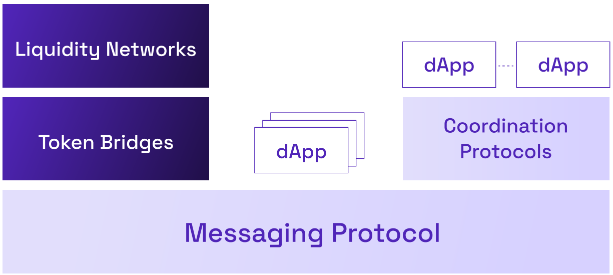


Fig. 3. Layers of cross-chain communication protocols [1]

well as Wormhole's Portal and external Carrier bridge. Before a more profound categorization of the systems, it, therefore, becomes clear that the prevalence of mutually independent solutions is significantly lower than assumed when the underlying messaging protocols are considered.

Let us focus on asset transfers, the most popular interoperability mode, typically realized by bridges, and inspect which types there are. Over the recent years, a consensus emerged within the industry regarding the classification of bridges according to the *Interoperability Trilemma - Trustlessness, Extensibility and Generalizability*. Informally, trustlessness means that the security of the bridge is directly pegged to the underlying (source) blockchain. Extensibility means the bridge can support additional blockchains without major refactoring. Generalizability means the bridge is capable of performing both data transfers and asset transfers.

The interoperability trilemma states there is a tradeoff between factors such as latency, cost, and security, implying that different bridge designs exist to accommodate each side of the spectrum. The bridge classification predicts different architectures, systems, and security models. Bridges can be classified into the categories natively, locally, optimistically, and externally verified [13–15, 21, 22, 28] (see Table 1). Indeed, the different categories represent different points in a *trust spectrum*. Typically, the higher the solution is in Table 1, the more "trustless" it is.

Having already implicitly addressed generalizability - the ability to process arbitrary data - and extensibility - the support of and effort required to expand an interoperability system with new chains - trustlessness undeniably represents the practically most important dimension, given the number of hacks and amount of damage already suffered by the space [10, 32, 33, 70]. Trustlessness - a measure for the additional trust required from users of an interoperability system beyond that in the underlying source and destination chains - is closely related to the solution's verification mechanism, potential further trust, and liveness assumptions, and together with these, it constitutes protocol-sided security. However, given the difficulty of reliably assessing highly complex systems with unique architectures, constantly changing maturity, and under permanent threat from a variety of risks and attack vectors [1, 53, 68], a new approach to trust in interoperability is to look at it as a spectrum [23]. Comparing LayerZero to some of the other most frequented protocols and solutions is our example to illustrate this [5, 27, 30, 31, 56, 75, 84].

LayerZero is a generic messaging protocol consisting of an endpoint on each source and destination chain and two types of off-chain actors that transmit different parts of the data required for the state synchronization necessary for interoperability between networks, oracle and relayer [89]. At first glance, it might appear like a natively verified bridge, in which, by definition, messages

Bridge Type	Description	Trust Assumptions	Trust Anchor	Example
Natively Verified	Destination chain independently verifies that the received state is valid and final according to the source network's state transition and consensus rule. Agents passing transaction proof and block header from source to destination chain where verification and conditional execution occurs (as long as transaction proof and header match). Alternatively, the destination chain can independently verify the received state chain. Light-client protocol of source chain I s ran on destination chain, with a smaller validator set.	Consensus from source chain is obtained and final	Source Chain	Light clients and relays: IBC, LayerZero, Rollups
Locally Verified	Similar to state channels, generally two parties involved verify each other's transaction during execution and settlement. They lock tokens on source/destination chains for a period of time with a dispute mechanism to facilitate cross-chain atomic swaps (HTLC). If the transction is abandoned, funds will be retrievable after the time period expires.	Consensus from source chain is obtained and final Hash functions used in the contracts are sound	2 of 2 Economic adversarial counter parties, involved chains, off-chain synchronization	Connext Legacy, Hop
Optimistically Verified	External validators (Attestors and Watchers) attest to the validity of cross-chain message from source to destination similar to Optimistic rollup. Attestors bond slashable funds on source chain and attest to new states (similar to Sequencer), while Watchers conduct fraud proof within a time window if invalid. 1 of N security model (relies on one honest actor)	At least one honest watcher	Honest fraud proof agent(s) Smart contracts enforcing slashing	Nomad, Hyperlane (optional)
Externally Verified	External validators, generally bonded, attest to the validity of cross-chain messages from source to destination. Hence, a threshold of honest validators (m of n) ensures the message protocol's safety and liveness. (multi-sig, consensus, threshold signature, SGX, etc.)	Off-chain consensus is done correctly	External validators	Wormhole, Axelar, Celer, Ronin, Hyperlane (options)

Table 1. Description of different bridge categories. Solutions upper in the table are considered more trustless (trust rooted on cryptographic mechanisms; while solutions more on the bottom rely more on more centralized anchors (e.g., multisg).

containing state changes to be replicated are signed by the source verifiers (or a committee thereof [54]), relayed cross-chain, checked for validity against the source protocol, and finally reproduced by the verifiers of the destination. Usually, this is achieved by, on the destination, implementing a smart-contract-based execution environment of the source, a so-called light client. While LZ's transaction cycle is similar to that in a light-client relay, unlike the trust-minimized natively verified IBC and XCMP, for sound functionality, the system relies on oracle and relayer not colluding to inject maliciously forged state change, which can be a bold assumption. The idea behind this design is that developers should be able to choose their security model based on the tradeoff between trustlessness and costs (including considerations about performance). This further trust assumption required by the relayer [86, 88] owed to the implicit on-demand compared to a cost-prohibitive explicit block header synchronization [92] undermines the system's Trustlessness and is reminiscent of an externally verified solution [65].

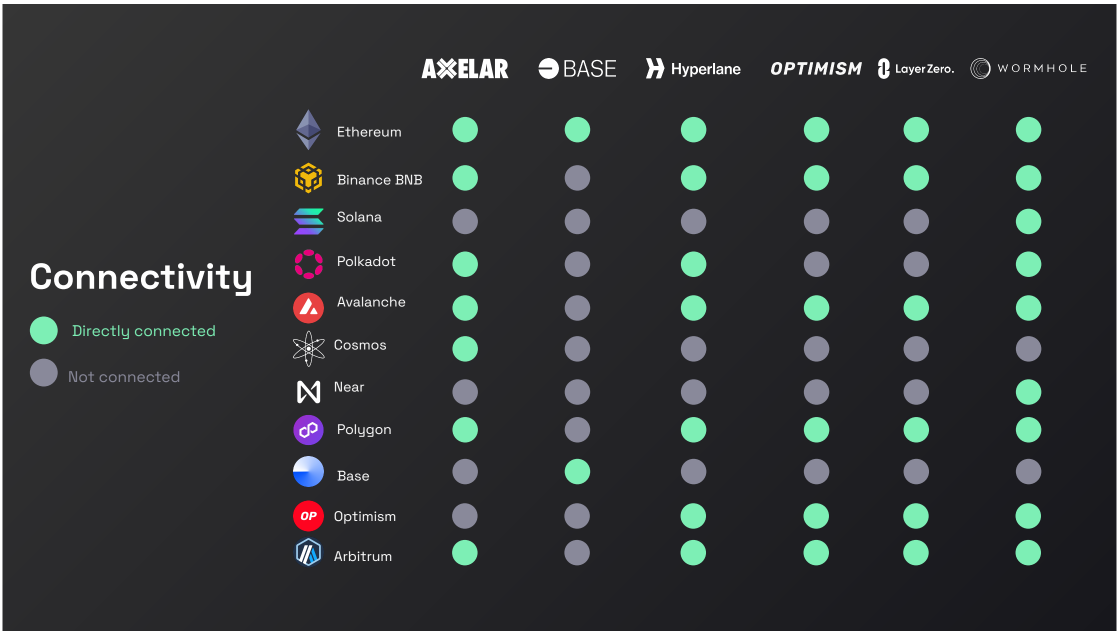
While the following is generally true of such systems but not of LZ, namely the existence of intermediary blockchains, cryptocurrencies, and verifiers that reach consensus on message validity and inclusion according to their own set of rules off-chain, users of applications that integrate LZ must still place additional trust in the interoperability solution. Although the services that perform system-critical tasks can be individually configured for each communication channel and both roles permissionlessly be covered by self-deployment, by default, Chainlink (a prestigious oracle network) and LZ are set as providers of oracle and relayer, respectively. Since evaluations are always to be based on the reference condition and weakest link - in this case, the relayer - it must be noted that LZ, like Wormhole, is a system that, at least, partially relies on social trust.

Even if additional measures are offered, such as application-specific security modules supplementing the default validator set, like in Hyperlane [51], multi-party computation on the consensus protocol's threshold signature scheme, like in Axelar [4], or a local copy of the destination chain used by the relayer to preemptively simulate cross-chain transactions off-chain and prevent malicious ones from being executed on-chain, *ante festum*, like in LayerZero [87] - it is virtually impossible for externally verified solutions to achieve the same trustlessness as systems of the other mechanisms. This becomes clearer when crypto-economic implications are considered. While at the current market capitalizations of Cosmos Hub and Polkadot, an attacker would need to mobilize approximately $1.5 billion and $3.25 billion, respectively, to corrupt the respective ecosystems or XCMP in a 51% attack - merely taking one side of the verification into account and assuming that control over 51% of the underlying capital is sufficient to take over a protocol, which it is not, as the technical hurdles and financial thresholds lie significantly higher - it would only require approximately $60 million in Axelar. Although not trust-minimized like natively verified solutions, Axelar is an insured system, meaning validators have to post a deposit to participate, which can be slashed and distributed to users in case of misbehavior, making an attack financially risky and thus less likely, according to game theory.

Between the extremes of the trust spectrum in externally verified systems, socially trusted and insured lie bonded solutions. Like insured systems, they require the staking of collateral; however in the event of misconduct, like in trusted systems, it is burned and not distributed to those affected in an attempt to compensate them at least partially. Chainlink and Polygon's PoS Bridge are two examples, although the former is not a sovereign token bridge. Within the verification mechanism spectrum, two more forms lie between the edges of externally and natively verified - optimistically and locally verified solutions. In locally verified systems such as liquidity-network-based Connext, the user interacts directly with the interoperability solution previously described for HTLCs, representing an important technical foundation for this category.

Even if additional measures are offered, such as application-specific security modules supplementing the default validator set, like in Hyperlane [51], multi-party computation on the consensus protocol's threshold signature scheme, like in Axelar [4], or a local copy of the destination chain used by the relayer to preemptively simulate cross-chain transactions off-chain and prevent malicious ones from being executed on-chain, *ante festum*, like in LayerZero [87] - externally verified solutions can not achieve the same trustlessness as systems of the other mechanisms. This becomes clearer when crypto-economic implications are considered. At the current market capitalizations of Cosmos Hub and Polkadot, an attacker would need to mobilize approximately $1.5 billion and $3.25 billion, respectively, to corrupt the respective ecosystems in an 51% attack. mBy merely taking one side of the verification into account and assuming that control over 51% of the underlying capital is sufficient to take over a protocol (which it is not as the technical hurdles and financial thresholds lie significantly higher) - it would only require approximately $60 million in Axelar. Although not trust-minimized like natively verified solutions, Axelar is an insured system, meaning validators have to post a deposit to participate, which can be slashed and distributed to users in case of misbehavior, making an attack financially risky and thus less likely, according to game theory.

Between the extremes of the trust spectrum in externally verified systems, socially trusted and insured lie-bonded solutions. Like insured systems, they require the staking of collateral; however, in the event of misconduct, like in trusted systems, it is burned and not distributed to those affected in an attempt to compensate them at least partially. Chainlink and Polygon's PoS Bridge are two examples, although the former is not a sovereign token bridge. Within the verification mechanism spectrum, two more forms lie between the edges of externally and natively verified - optimistically and locally verified solutions. In locally verified systems such as liquidity-network-based Connext, the user interacts directly with the interoperability solution previously described for HTLCs, representing an important technical foundation for this category. In terms of security, the user, therefore, only has to trust open-source cryptography and their financial interest, which is adverse to the bridges.



Connectivity

🟢 Directly connected

⚪ Not connected

	AXELAR	BASE	Hyperlane	OPTIMISM	LayerZero.	WORMHOLE
Ethereum	🟢	🟢	🟢	🟢	🟢	🟢
Binance BNB	🟢	⚪	🟢	🟢	🟢	🟢
Solana	⚪	⚪	⚪	⚪	⚪	🟢
Polkadot	🟢	⚪	🟢	⚪	⚪	🟢
Avalanche	🟢	⚪	🟢	🟢	🟢	🟢
Cosmos	🟢	⚪	⚪	⚪	⚪	⚪
Near	⚪	⚪	⚪	⚪	⚪	🟢
Polygon	🟢	⚪	🟢	🟢	🟢	🟢
Base	⚪	🟢	⚪	⚪	⚪	⚪
Optimism	⚪	⚪	🟢	🟢	🟢	🟢
Arbitrum	🟢	⚪	🟢	🟢	🟢	🟢

Fig. 4. Mapping between popular interoperability solutions and supported ecosystems.

2.2 Current obstacles and challenges

There are many ongoing challenges in interoperability, many of which are systematized in [9, 12]. The ones we believe are the most prominent as of June 2023 are privacy, benchmarking, and security monitoring. An orthogonal problem in the area is the lack of uniformization of terms and vocabulary: the academia and industry speak different languages in this research area. Therefore, we put forward, available in the online appendix, an extensive vocabulary that joins both worlds, the outcome of a research project at Blockdaemon. It is available online [3].

2.2.1 Cross-chain privacy. It is generally agreed upon that the properties of anonymity (in terms of unlinkability), confidentiality, and indistinguishability of transactions are beneficial privacy properties in the cross-chain context [85]. An anonymous asset transfer (or exchange) will hide the identities of the parties involved in the transfer. Confidentiality will hide the number of transferred tokens. Indistinguishability means an external observer cannot say whether or not the transaction is part of a swap. Researchers and practitioners alike have done work in cross-chain, specifically in the areas of asset transfers (namely between privacy-enhanced blockchains, as the source, and public blockchains, as the target [71], leveraging promising technologies such as zero-knowledge proofs). Although there is a long way ahead, existing work seems to suggest that in scenarios where at least one confidential blockchain is involved (by confidential, we mean permissioned or privacy-enabled by default like Hyperledger Fabric, ZCash, or Monero, e.g., confidential to confidential), preserving the property of unlinkability is possible, therefore achieving some level of anonymity (and possible some confidentiality depending on the blockchain, as ZCash would allow). Privacy on asset exchanges has also been studied [34] (see, for example, an implementation of a cross-chain private asset exchange here[4]). Privacy on asset exchanges looks more straightforward

[3] https://l2-interop-glossary-blockdaemon-research-develop-a28a37cf925a12.gitlab.io/
[4] https://github.com/RafaelAPB/blockchain-integration-framework/tree/private-htlcs

than other interoperability modes: HTLCs share secrets only understandable by the involved parties, so it becomes harder to draw direct associations between transactions. Of course, by analyzing certain heuristics (simpler: amount locked, cryptographic parameters such as the prime field for a private HTLC; more complex: time intervals for swaps, user activity interactions, crossing with off-chain data) one could de-anonymize the actors behind cross-chain transactions. Thus, more research is needed.

On the other hand, privacy on data transfers is studied only partially: some authors worked on the concept of self-sovereign identity to facilitate cross-chain interactions [8, 42]. In fact, interoperation for data sharing between blockchains requires the networks' ability to authenticate requests using well-defined access control policies (and thus increasing confidentiality) and validating proofs. While the first steps have been taken, no practical implementations of this idea exist. Furthermore, to the best of our knowledge, no empirical studies are studying cross-chain privacy. We emphasize that there is a trade-off between privacy and accountability: revocation of privacy could be conditional (e.g., the user moves funds above the established limit), dependent on the interoperability mechanism architecture.

2.2.2 Interoperability Solution Benchmark. Multiple benchmarking efforts and standardization efforts are in progress. However, there are still considerable challenges since the lack of a uniform API and concrete benchmark datasets hinders a systematic comparison between cross-chain systems (although directions for evaluating interoperability solutions already exist [9, 62]) and a few interoperability solutions are assessed in detail [24]. Methodology and empirical studies to assess components around cross-chain solutions, such as cryptographic primitives, libraries, compilers (especially relevant for SNARK or STARK-based solutions [52]), SDKs, and hardware accelerators, among others, need to be further developed. Studying interoperability solutions in the Web3 world will also give back to traditional interoperability research, as we collect insights on integrating centralized with decentralized systems. There is industry interest to study this topic[5].

2.2.3 Security Monitoring. Monitoring bridges and the sophisticated, and sometimes fragile relationships between ecosystems quickly becomes hard, because the systems to be dealt with are heterogeneous and decentralized, and the systems built on top of them (e.g., decentralized applications) may have arbitrarily complex business logic [10]. Imagine a simple case: your application on blockchain A depends on the consensus of blockchain B. What happens if blockchain B forks, is attacked (e.g., 51%), suffers any of the many possible cross-chain attacks [59], or even collapses?

This last possibility was a reality for the Terra blockchain, with implications for the Cosmos and Ethereum ecosystem, as they were connected by the Osmosis bridge. In the Terra blockchain collapse, exploiters created a destabilization of the stablecoin hosted by Terra. This destabilization caused liquidation cascading, possibly the main cause for a new crypto crash [35]. The collapse of economic security on Luna posed dangers for the Cosmos hub Osmosis, a decentralized exchange bridged to Ethereum. In Osmosis, there was $66 million dollars of OSMO tokens in the UST/OSMO pool, where UST is the Terra blockchain, that could be stolen over the bridge by an attacker with voting power equal to two-thirds of the staked LUNA. A solution to this problem was for bridge operators to manually shut down bridges, causing impermanent losses. The monitoring of the operations underlying this particular use case could have prevented such a tragic outcome and helped mitigate loss. In a cross-chain setting, automating the discovery of cross-chain models and enabling their monitoring becomes very challenging, as there is a lack of tools to secure and monitor cross-chain applications. Solutions based on modeling by specification [10] or based on large language models [39] could be interesting directions for future work.

[5] https://wiki.hyperledger.org/display/INTERN/Benchmarking+Cross-Chain+Bridges

Category	Challenge	Progress	Notes	Reference
Theory/ Systematization	Interoperability Model	◐	Needs provable security model	[1, 9, 12, 53]
	Representing Cross-Chain State	●	Via, e.g., blockchain views	[10]
	Standardization (technical, semantic)	●	Multiple protocols that are maturing	[58]
	Standardization (organizational, legal)	◐	Several initiatives in bootstrapping phase	[47]
Scalability	Sidechains for scale (rollups)	◐	Sidechains are mature at this point, but more research is needed for extra scale	[7]
	Succint arguments of knowledge-based approaches for performant interoperability	◐	New research area with applications to scalable interoperability	[41, 52]
Multi-chain and Cross-chain	Homogeneous interoperability within blockchain engines	◐	Not all blockchain engines have reached the maturity stage	[12]
	Bridges across blockchain engines	◐	Some projects tackle this, but still not matured	[4, 21, 28]
	Increase resiliency to attacks (e.g., standardizing incident responses processes)	◐	Adhoc mechanisms in place that lack a clearly defined process and documentation	[10, 12]
Processes and Monitoring	Systematic interoperability benchmarks	◐	Few solutions systematically evaluated, lack of benchmarks	[24, 62]
	Modelling and visualization of cross-chain state	◐	Fine-grain monitoring implemented, lacking state visualization	[10]
	Advanced secure monitoring (e.g., cross-chain models, large language models)	◐	First PoCs done, more research needed	[10, 39]
Privacy	General privacy-preserving interoperability solutions (data transfers)	○	Work need to be done on anonymity and confidentiality	[85]
	Privacy-preserving asset exchanges	●	HTLCs can provide indistinguishably and unlinkeability	[34, 85]
	Privacy-preserving asset transfers	◐	Work need to be done on anonymity and confidentiality	[71, 85]

Table 2. Current date evaluation of open-ended challenges and research questions regarding blockchain interoperability posed in 2021, as of June 2023. ● - mostly addressed; ◐ - partially addressed; ○ - not addressed or addressed insufficiently.

Table 2 shows the open challenges and research directions in 2021 [12] vs. the *status quo* (June 2023). Another fundamental challenge is the lack of a theory of interoperability that can provide a reasoning framework to the different interoperability techniques, modes, and associated workflows - making practitioners have a difficult time understanding and analyzing the properties and scope of interoperability solutions, and even harder to compare them [62]. Some pressing questions when evaluating interoperability frameworks are: *what are the DLTs cryptographic mechanisms that facilitate secure and private interoperability?*, and *what are the security and privacy trade-offs of different interoperability solutions, versus performance and cost?*

3 THE ROAD AHEAD FOR INTERCONNECTED HYBRID INFRASTRUCTURES

There are a number of trade-offs that practitioners consider when designing their solutions. Such trade-offs inform a number of key trends emerging from the industry, mirroring those in the Layer 1 network realm. The first one is modular stack design, and hence the emergence of *omnichain applications*. Omnichain applications (also known as multiple chain decentralized applications [9]) are applications utilizing different chains. Instead of having a single interoperability solution to handle all the functions similar to a monolithic Layer 1 network, we observe that blockchain interoperability solutions are increasingly specialized to handle secure arbitrary message passing at a lower level, value transfer, and coordination of remote state-dependent transactions at a higher level[1]. Such a stack framework allows developers to offload the security component to GMPs while focusing on developing omnichain applications, dApps that coordinate dependent transactions across two or more networks such as cross-chain *decentralized exchanges* (DEXs), also called DEX aggregators. Sushiwap and Stargate Finance on LayerZero, Squid Router on Axelar, and Osmosis on IBC are examples of cross-chain DEXes enabled by different interoperability solutions.

The second trend is security-driven model selection. Similar to lower value transactions migrating to Ethereum layer 2 solutions while higher value ones that demand more security remain on the main chain, the selection of particular security models for cross-chain dApps will be largely determined by the use cases and the level of trust and risk the users are able to tolerate. Each model has a clear set of trade-offs in statefulness, security, capital efficiency, speed, and connectivity[13]. For instance, use cases that prioritize speed and cost with lower security requirements can utilize the external multi-sig model while those that prioritize security with lower requirements on speed can utilize the optimistic model[50] or SNARKs [52]. Security here is also tied with the notion of finalization: cross-chain transactions should be considered settled once a reasonable finalization time in the slowest blockchain has passed. In any case, there should be a plan that accounts for network-consensus risks (e.g., transactions being reverted, chain halting, 51% attacks).

The third trend is the potential consolidation of GMPs similar to the consolidation in layer 1 networks (see for example [37]) with most transactions happening on Ethereum, Avalanche, Cosmos, BSC, Solana, and others. There are several contributing factors such as fragmented liquidity and network effect. On fragmented liquidity, many monolithic solutions utilize different wrap versions of the same asset on the destination chain, resulting in low depth in liquidity pools and hence sub-optimal trading and liquidity provision experience. Such a problem could propel users to migrate to solutions with more adoption across the stack for a better experience and lower capital loss, hence the network effect. From what we have observed, it will be quite likely for different blockchain ecosystems to have canonical interoperability solutions that connect to other ecosystems. It could be asset specific such as Circle's Cross-Chain Transfer Protocol for USDC stablecoin, chain-specific such as Evmos connecting Cosmos Ecosystem to Ethereum, or highly generalized solutions, such as LayerZero for GMPs. In addition, we envision one possible scenario of further specialization in functions across the solution stack accompanying a diminishing presence of monolithic solutions, because modular solutions off-load lower-level work and offer options and flexibility for developers, while providing a more unified experience for the end users as GMP layer consolidates. In this scenario, there could be a smaller number of GMPs with a large number of omnichain applications and a reasonable amount of token bridges and liquidity networks built on top, mirroring the Layer 1 landscape.

The fourth trend is the tendency for users and businesses to use bridge aggregators for asset transfers. Bridge aggregators expose several existing bridges in a single interface, that can provide a better user experience, by systematically and explicitly providing details about cross-chain transaction latency, cost, and throughput, and even visualizing the cross-transaction flow [10]. The end user would be able to choose from a range of options depending on their specific needs, availability of liquidity, and connectivity. The key idea is to provide an easy range of alternatives if a bridge (or ecosystem) is attacked, enhancing the connectivity capabilities of the non-expert Web3 user, especially when one needs to analyze and decide upon the technical specifications, security, and network models, as well as constant upgrades of over a hundred bridge solutions. The trend is analogous to node providers such as Blockdaemon taking in the complexity of managing the analysis, deployment, and maintenance of hundreds of different blockchain protocols on behalf of their clients. Although seemingly a positive trend, bridge aggregators add a layer of complexity and contribute to a larger attack surface. They, by construction, inherit the bridge's shortcomings and current challenges (e.g., do they leverage monitoring tools to check up on the current state of a transaction? How to mitigate potential transaction failure coming, for example, of wrong gas price estimates or slippage?). An alternative to bridge aggregators would be using security-enhancing mechanisms by combining multiple different sources of (block-hash) truth for enhanced security (see Gnosis Hashi).

4 KEY TAKEAWAYS

Recent developments in blockchain have been incredibly exciting, unveiling a realm of possibilities that were not possible ten years ago. We identified four trends shaping today's interconnected blockchain ecosystems: the adoption of modular stack designs, driven security model selection, consolidation of GMPs, and usage of bridge aggregators. Indeed, there are few doubts that these technologies will cause fundamental changes in how we interact with each other, and how we perceive and exchange knowledge. In spite of its weaknesses, particularly the high computational cost in terms of latency and resources, blockchain is likely to remain an important component for decentralizing our society. However, its full potential needs to be unlocked via synergies with centralized and other decentralized systems. Among the multiple tasks to be done, work on enhancing the privacy of cross-chain solutions, creating benchmarks to assess cross-chain systems, and monitoring are the most important ones. We call for a joint endeavor from researchers, engineers, and data and privacy experts as an essential vehicle to unlocking the potential of blockchain for the world at large.

ACKNOWLEDGMENTS

We warmly thank André Augusto, Jonas Pfannschmidt, Chris Spannos, Freddy Zwanzger, Andie Baker, Dom Martinez, Gabriel Crispino, the colleagues at Hyperledger Cacti, and our colleagues in the IETF's working group Secure Asset Transfer Protocol (SATP) for fruitful discussions. This work was partially supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UIDB/50021/2020 (INESC-ID) and 2020.06837.BD. Rafael was supported by a Fulbright Scholarship while doing research at MIT Connection Science (MIT Media Lab), and Blockdaemon.

REFERENCES

[1] Abebe, Ermyas and Robinson, Peter and Chand, Arjun and Murdock, Mark and Hyland-Wood, David. Crosschain Risk Framework, 2023. Available online: https://crosschainriskframework.github.io/, last accessed on 2023-05-21.

[2] Alpern, B., and Schneider, F. B. Defining liveness. *Information processing letters 21*, 4 (1985), 181–185.

[3] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (2018), pp. 1–15.

[4] Axelar Team. Axelar Network: Connecting Applications with Blockchain Ecosystems, 2021. Available online: https://axelar.network/axelar_whitepaper.pdf, last accessed on 2023-05-22.

[5] Axelar Team. Axelarscan, 2021. Available online: https://axelarscan.io/, last accessed on 2023-05-22.

[6] Axelar Team. What Is General Message Passing and How Can It Change Web3?, 2022. Available online: https://axelar.network/blog/general-message-passing-and-how-can-it-change-web3, last accessed on 2023-05-21.

[7] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., and Wuille, P. Enabling blockchain innovations with pegged sidechains. *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains 72* (2014), 201–224.

[8] Belchior, R., Putz, B., Pernul, G., Correia, M., Vasconcelos, A., and Guerreiro, S. Ssibac: self-sovereign identity based access control. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (2020), IEEE, pp. 1935–1943.

[9] Belchior, R., Riley, L., Hardjono, T., Vasconcelos, A., and Correia, M. Do you need a distributed ledger technology interoperability solution? *Distributed Ledger Technologies: Research and Practice 2*, 1 (2023), 1–37.

[10] Belchior, R., Somogyvari, P., Pfannschmid, J., Vasconcelos, A., and Correia, M. Hephaestus: Modelling, analysis, and performance evaluation of cross-chain transactions. *TechRxiv preprint* (2023). Available at: https://www.techrxiv.org/articles/preprint/Hephaestus_Modelling_Analysis_and_Performance_Evaluation_of_Cross-Chain_Transactions/20718058.

[11] Belchior, R., Vasconcelos, A., Correia, M., and Hardjono, T. Hermes: Fault-tolerant middleware for blockchain interoperability. *Future Generation Computer Systems 129* (2022), 236–251.

[12] Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. A survey on blockchain interoperability: Past, present, and future trends. *ACM Computing Surveys (CSUR) 54*, 8 (2021), 1–41.

[13] Berenzon, Dmitriy. Blockchain Bridges: Building Networks of Cryptonetworks, 2021. Available online: https://medium.com/1kxnetwork/blockchain-bridges-5db6afac44f8, last accessed on 2023-05-21.

[14] Bhuptani, Arjun. The Interoperability Trilemma: AKA Why Bridging Ethereum Domains is So Damn Difficult, 2021. Available online: https://blog.connext.network/the-interoperability-trilemma-657c2cf69f17, last accessed on 2023-05-21.

[15] Bhuptani, Arjun. Optimistic Bridges: A New Paradigm for Crosschain Communication, 2022. Available online: https://blog.connext.network/optimistic-bridges-fb800dc7b0e0, last accessed on 2023-05-21.

[16] Blockdaemon. Platform - Blockdaemon, 2021. Available online: https://blockdaemon.com/platform/, last accessed on 2022-01-10.

[17] Blockdaemon. Blockdaemon's universal api, 2023. Available online: https://docs.blockdaemon.com/reference/universal-api-overview (Accessed on 11 May 2023).

[18] Buterin, V. vitalik.eth on twitter, arguments for a multi-chain future, 2022. Available online: https://twitter.com/VitalikButerin/status/1479501366192132099 (Accessed on 11 May 2023).

[19] Buterin, V., et al. A next-generation smart contract and decentralized application platform. *white paper 3*, 37 (2014), 2–1.

[20] Chainspot. Find your bridge with the largest blockchain bridges aggregator, 2021. Available online: https://chainspot.io/, last accessed on 2023-05-21.

[21] Chand, Arjun. Navigating Arbitrary Messaging Bridges: A Comparison Framework: Axelar vs. LayerZero vs. Nomad vs. Wormhole vs. Celer IM vs. anyCall vs. Hyperlane vs. deBridge, 2022. Available online: https://blog.li.fi/navigating-arbitrary-messaging-bridges-a-comparison-framework-8720f302e2aa, last accessed on 2023-05-21.

[22] Chand, Arjun. What Are Blockchain Bridges And How Can We Classify Them? Classifying Bridges As We Know Them, 2022. Available online: https://blog.li.fi/what-are-blockchain-bridges-and-how-can-we-classify-them-560dc6ec05fa, last accessed on 2023-05-21.

[23] Chand, Arjun. With Bridges, Trust is a Spectrum, 2022. Available online: https://blog.li.fi/li-fi-with-bridges-trust-is-a-spectrum-354cd5a1a6d8, last accessed on 2023-05-21.

[24] Chervinski, J. O., Kreutz, D., Xu, X., and Yu, J. Analyzing the performance of the inter-blockchain communication protocol. *arXiv preprint arXiv:2303.10844* (2023).

[25] Coindesk. Cross chain articles - coindesk, 2023. Available online: https://www.coindesk.com/tag/cross-chain/ (Accessed on 11 May 2023).

[26] CoinTelegraph. Why interoperability is the key to blockchain technology's mass adoption, 2023. Available online: https://cointelegraph.com/news/why-interoperability-is-the-key-to-blockchain-technology-s-mass-adoption (Accessed on 11 May 2023).

[27] Connext. Connextscan, 2021. Available online: https://connextscan.io/, last accessed on 2023-05-22.

[28] Connext. Welcome! | Connext Documentation, 2021. Available online: https://docs.connext.network, last accessed on 2021-08-10.

[29] Correia, M. From Byzantine Consensus to Blockchain Consensus. *Essentials of Blockchain Technology* (2019), 41.

[30] DefiLlama. Bridge TVL Rankings, 2020. Available online: https://defillama.com/protocols/Bridge, last accessed on 2023-05-22.

[31] DefiLlama. Bridge Volume in all bridges, 2020. Available online: https://defillama.com/bridges, last accessed on 2023-05-22.

[32] Derka, Martin. ETHDenver 2022: EVM-to-EVM chain bridges: The Good, The Bad, and The Ugly, 2022. Available online: https://www.youtube.com/watch?v=Oa-b6mROCeI, last accessed on 2023-05-22.

[33] Derka, Martin and Murashkin, Alex and Bak, Kacper and Lee, Sung-Shine. ETHDenver 2023: How to Hack a Bridge in 2022, 2023. Available online: https://www.youtube.com/watch?v=Oa-b6mROCeI, last accessed on 2023-05-22.

[34] Deshpande, A., and Herlihy, M. Privacy-preserving cross-chain atomic swaps. In *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers* (2020), Springer, pp. 540–549.

[35] Economy, and Business. Luna crypto crash wipes out savings of thousands of investors, sparking fears for sector | economy and business | el paÍs english, 2022. Available online: https://english.elpais.com/economy-and-business/2022-05-12/luna-crypto-crash-wipes-out-savings-of-thousands-of-investors-sparking-fears-for-sector.html, last accessed on 2023-05-25.

[36] Ethereum Developer Docs Contributors. Developer Docs: Bridges, 2022. Available online: https://ethereum.org/en/developers/docs/bridges/, last accessed on 2023-05-21.

[37] Expand Network. Expand Network - Web3 development platform for multichain solutions, 2023. Accessed on 8 June 2023.

[38] Fan, X., Chai, Q., and Zhong, Z. Multav: A multi-chain token backed voting framework for decentralized blockchain governance. In *Blockchain–ICBC 2020: Third International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 3* (2020), Springer, pp. 33–47.

[39] Gai, Y., Zhou, L., Qin, K., Song, D., and Gervais, A. Blockchain large language models. *arXiv preprint arXiv:2304.12749* (2023).

[40] Garay, J., Kiayias, A., and Leonardos, N. The Bitcoin backbone protocol: Analysis and applications. In *Advances in Cryptology* (2015), vol. 9057, pp. 281–310.

[41] Garoffolo, A., Global Horizen, A., Kaidalov, D., and Oliynykov, R. Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. *2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)* (2020).

[42] Ghosh, B. C., Ramakrishna, V., Govindarajan, C., Behl, D., Karunamoorthy, D., Abebe, E., and Chakraborty, S. Decentralized cross-network identity management for blockchain interoperation. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2021), IEEE, pp. 1–9.

[43] Gilbert, S., and Lynch, N. Perspectives on the cap theorem. *Computer 45*, 2 (2012), 30–36.

[44] Giulio, C. Before ethereum. the origin and evolution of blockchain oracles. *IEEE Access* (2023), 1–1.

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

[46] Hardjono, T., Lipton, A., and Pentland, A. Toward an interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management 67*, 4 (2019), 1298–1309.

[47] Hargreaves, M., Hardjono, T., and Belchior, R. Secure Asset Transfer Protocol (SATP).

[48] Heflin, J., and Hendler, J. Semantic interoperability on the web. Tech. rep., Maryland Univ College Park Dept of Computer Science, 2000.

[49] Herlihy, M. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing* (2018), pp. 245–254.

[50] Hyperlane. Docs: Introduction, 2022. Available online: https://docs.hyperlane.xyz/docs/introduction/getting-started, last accessed on 2023-05-21.

[51] Hyperlane. Docs: Validators, 2022. Available online: https://docs.hyperlane.xyz/docs/protocol/agents/validators, last accessed on 2023-05-22.

[52] Ivanichkov, E., Dimov, D., Armenchev, S., Miladinov, Y., Kirkov, K., Kirov, P., Karadjov, Z., and Belchior, R. Dendreth: Ethereum snark-based beacon light client for multiple blockchain ecosystems.

[53] Kiepuszewski, Bartek and Chellani, Vaibhav. L2Bridge Risk Framework 2.0, 2022. Available online: https://gov.l2beat.com/t/l2bridge-risk-framework/31/1, last accessed on 2023-05-21.

[54] Kissling, Etan. Ethereum Proof-of-Stake Consensus Altair Upgrade Light Client Specifications, 2022. Available online: https://github.com/ethereum/consensus-specs/tree/dev/specs/altair/light-client, last accessed on 2023-05-22.

[55] Kwon, J., and Buchman, E. Cosmos whitepaper. *A Netw. Distrib. Ledgers* (2019), 27.

[56] L2BEAT. Bridges, 2021. Available online: https://l2beat.com/bridges/tvl, last accessed on 2023-05-22.

[57] LaVean, G. Interoperability in defense communications. *IEEE transactions on communications 28*, 9 (1980), 1445–1455.

[58] LayerZero. Docs: Oracle, 2021. Available online: https://layerzero.gitbook.io/docs/ecosystem/oracle, last accessed on 2023-05-23.

[59] Lee, S.-S., Murashkin, A., Derka, M., and Gorzny, J. Sok: Not quite water under the bridge: Review of cross-chain bridge hacks. *arXiv preprint arXiv:2210.16209* (2022).

[60] Manyika, J., and Roxburgh, C. The great transformer: The impact of the internet on economic growth and prosperity. *McKinsey Global Institute 1*, 0360-8581 (2011).

[61] Markey-Towler, B. Anarchy, blockchain and utopia: A theory of political-socioeconomic systems organised using blockchain. *Available at SSRN 3095343* (2018).

[62] Mihaiu, I., Belchior, R., Scuri, S., and Nunes, N. A framework to evaluate blockchain interoperability solutions. *TechRxiv preprint* (2021). Available at: https://www.techrxiv.org/articles/preprint/A_Framework_to_Evaluate_Blockchain_Interoperability_Solutions/17093039/2.

[63] Montgomery, H., Borne-Pons, H., Hamilton, J., Bowman, M., Somogyvari, P., Fujimoto, S., Takeuchi, T., Kuhrt, T., and Belchior, R. Hyperledger cactus whitepaper.

[64] Nakamoto, S. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* (2008).

[65] Nandini, Eshita. IBC Outside of Cosmos: The Transport Layer, 2023. Available online: https://messari.io/report/ibc-outside-of-cosmos-the-transport-layer, last accessed on 2023-05-22.

[66] Narayanam, K., Ramakrishna, V., Vinayagamurthy, D., and Nishad, S. *Atomic cross-chain exchanges of shared assets.* Feb 2022. ADS Bibcode: 2022arXiv220212855N type: article.

[67] Narayanam, K., Ramakrishna, V., Vinayagamurthy, D., and Nishad, S. Atomic cross-chain exchanges of shared assets. *arXiv preprint arXiv:2202.12855* (2022).

[68] Nomad. Nomad Docs: Security, 2022. Available online: https://docs.nomad.xyz/the-nomad-protocol/security, last accessed on 2023-05-21.

[69] Pillai, B., Biswas, K., Hóu, Z., and Muthukkumarasamy, V. Cross-blockchain technology: integration framework and security assumptions. *IEEE Access 10* (2022), 41239–41259.

[70] REKT. Leaderboard, 2020. Available online: https://rekt.news/leaderboard/, last accessed on 2023-05-21.

[71] Sanchez, A., Stewart, A., and Shirazi, F. Bridging sapling: Private cross-chain transfers. In *2022 IEEE Crosschain Workshop (ICBC-CROSS)* (2022), IEEE, pp. 1–9.

[72] Schwarz, Colin. ChainSafe Building ChainBridge: A Multi-Chain Arbitrary Message Passing Standard, 2020. Available online: https://blog.chainsafe.io/chainsafe-building-chainbridge-49d51ff2e0a2, last accessed on 2023-05-21.

[73] Shrimali, B., and Patel, H. B. Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University-Computer and Information Sciences 34*, 9 (2022), 6793–6807.

[74] Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., and Choo, K.-K. R. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications 149* (2020), 102471.

[75] Stargate Finance. Protocol Overview, 2021. Available online: https://stargate.finance/overview, last accessed on 2023-05-22.

[76] Tas, E. N., Han, R., Tse, D., Yu, F., and Nazirkhanova, K. Interchain timestamping for mesh security. *arXiv preprint arXiv:2305.07830* (2023).

[77] The Block. The block news - cross chain, 2023. Available online: https://www.theblock.co/search?query=cross%20chain (Accessed on 11 May 2023).

[78] Thibault, L. T., Sarry, T., and Hafid, A. S. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access* (2022).

[79] Traiger, I. L., Gray, J., Galtieri, C. A., and Lindsay, B. G. Transactions and Consistency in Distributed Database Systems. *IBM Research Report RJ2555* (1979).

[80] Wang, G., Shi, Z. J., Nixon, M., and Han, S. Sok: Sharding on blockchain. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* (2019), pp. 41–61.

[81] Wegner, P. Interoperability. *ACM Computing Surveys (CSUR) 28*, 1 (1996), 285–287.

[82] Westerkamp, M., and Küpper, A. Smartsync: Cross-blockchain smart contract interaction and synchronization. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2022), IEEE, pp. 1–9.

[83] Wood, G. Polkadot: Vision for a heterogeneous multi-chain framework. *White paper 21*, 2327 (2016), 4662.

[84] Wormhole. Portal Bridge Stats, 2020. Available online: https://www.portalbridge.com/#/stats, last accessed on 2023-05-22.

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

[86] Zarick, Ryan. LayerZero- An Omnichain Interoperability Protocol, 2021. Available online: https://medium.com/layerzero-official/layerzero-an-omnichain-interoperability-protocol-b43d2ae975b6, last accessed on 2023-05-22.

[87] Zarick, Ryan. Introducing: Pre-Crime, 2022. Available online: https://medium.com/layerzero-official/introducing-pre-crime-49bef4a581d5, last accessed on 2023-05-22.

[88] Zarick, Ryan. LayerZero Glossary, 2022. Available online: https://layerzero.gitbook.io/docs/faq/glossary, last accessed on 2023-05-22.

[89] Zarick, Ryan and Pellegrino, Bryan and Banister, Caleb. LayerZero: Trustless Omnichain Interoperability Protocol, 2021. Available online: https://layerzero.network/pdf/LayerZero_Whitepaper_Release.pdf, last accessed on 2023-05-22.

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

[91] Zhang, S. The design principle of blockchain: An initiative for the sok of soks. *arXiv preprint arXiv:2301.00479* (2023).

[92] Zhang, Isaac. LayerZero as an IBC Transport Layer, 2021. Available online: https://medium.com/layerzero-official/layerzero-as-an-ibc-transport-layer-5a676fd2a446, last accessed on 2023-05-22.

[93] Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., Qin, K., Wattenhofer, R., Song, D., and Gervais, A. Sok: Decentralized finance (defi) attacks. *Cryptology ePrint Archive* (2022).