# A Brief History of Blockchain Interoperability

Rafael Belchior[1], Jan Süßenguth[2], Qi Feng[2], Thomas Hardjono[2], André Vasconcelos[2], and Miguel Correia[2]

[1]INESC-ID
[2]Affiliation not available

April 02, 2024



**Abstract**

Blockchain interoperability conflates the need for distributed systems to communicate with third- party systems without the existence of a canonical chain or orchestration layer. As there is not "a chain to rule them all" (due to reasons such as 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 [13, 15, 16, 31], oracles [45], and other interoperability mechanisms [4, 9, 17, 48, 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.

# 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

CCS Concepts: • **Computer systems organization → Dependable and fault-tolerant systems and networks**.

**ACM Reference Format:**
Rafael Belchior, Jan Süßenguth, Qi Feng, Thomas Hardjono, André Vasconcelos, and Miguel Correia. 2024. A Brief History of Blockchain Interoperability. *J. ACM* 37, 4, Article 111 (August 2024), 10 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

*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* [15], *oracles* [27], and other *interoperability mechanisms* [9, 29, 48]. 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 [38], 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 work been done in the last decade (the past), how it is currently deployed and used in practice (the present), and likely paths of development (the future).

## 1 INTEROPERABILITY AS A DRIVER OF EVOLUTION

The world is rapidly changing. The current socio-economic environment, including rapid digitization of information and processes, the rise of machine learning, and ubiquitous access to the Internet, 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

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.




0004-5411/2024/8-ART111 $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

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. 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.

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. Such systems provide *safety* and *liveness*, 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*) [21]. 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* [37], 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, chain growth, and chain quality properties [25], meaning that, at a high level, honest nodes share a common history of blocks; the chain grows; 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. 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.

The blockchain trilemma, postulated by one of Ethereum's founders, states that blockchains have an inherent trade-off between security, scalability, and decentralization. Being an equivalent of the CAP theorem [26] 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 [21]). 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 - The Past

"Interoperability is the ability of two or more software components to cooperate despite differences in language, interface, and execution platform" [45]. Counting with a large corpus of research, interoperability has been studied since the 1980s [34], when engineers started observing the rise of complex software systems that communicated with other systems, heterogeneous in nature. Indeed, interoperability research tends to appear in a later stage of a given technology when modularity, composability, and heterogeneity come into play. As a natural evolution of technological advance, interoperability started gaining more notoriety with the emergence of the Internet [28]. 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. 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 [28]. Given the history of the development of the Internet and computer networks in general, it is not surprising that communities are pushing toward cross-chain interoperability. Consequently, the world is settling on several multi-chain blockchains connected by cross-chain solutions (typically bridges, considered major players in DeFi ecosystems) that are executed by cross-chain transactions. Cross-chain transactions are sets of local transactions that respect a set of business rules or conditions over several domains. Those conditions are called the cross-chain rules [11]. In practice, the 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 respect a set of properties equivalent to ACID [14], but with several fundamental limitations regarding atomicity. While atomicity states that either all the local transactions are executed correctly and committed to the underlying ledger, or none are, they are not guaranteed by default at the cross-chain level. 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?*.

One of the first attempts to solve the interoperability problem was to transfer assets between blockchains via atomic swaps [30], in 2012 [35], or 2013 [39]. Atomic swaps involve releasing locked assets in one chain upon a certain time period (i.e., using a timelock), a condition contingent upon the counterparty providing a secret. The first party can use this secret to reclaim tokens on the other blockchain. On the other hand, data transfers and interoperability with non-blockchain infrastructure started with the conceptualization, implementation, and academic study of oracles, around 2011, 2014, and 2020, respectively[2, 27]. Although data interoperability was considered first than asset interoperability, the latter problem was the focus of attention by blockchain communities due to its market interest. Crossing this information with [9, 15], we can conclude that the area of blockchain interoperability started to get traction around 2016-2017 (when number of yearly published papers on the topic exceeded ten documents [15], and there was enough interest to justify a survey of available solutions [17]).

### 1.2 Interoperability as a Requirement of Scalability of Service

Interoperability was initially studied in the scope of Bitcoin. With the appearance of new blockchains and supporting infrastructure, the scope increased: interoperability was quickly found to be a sensitive vehicle to off-load computation. Practitioners and researchers had to solve the caveat that this new type of interoperability had not to sacrifice decentralization and, simultaneously, achieve 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.

In light of the wide scope of interoperability, we can decompose it into two types: *multi-chain interoperability*, and *cross-chain interoperability*. In multi-chain interoperability, instances of a *blockchain of blockchains* framework [15], (e.g., Cosmos, Polkadot, Avalanche) communicate with each other through a trust anchor implemented in the protocol. Each instance has a built-in interoperability protocol and data format that other blockchains instantiated by the same framework understand. Consider Polkadot's instantiations called parachains: each parachain communicates

with other parachains via XCMP, a built-in interoperability format [46]. Communications are anchored by the canonical blockchain (the relay chain in Polkadot). In Cosmos, instances are called zones, which communicate via a protocol called Inter Blockchain Communication (IBC) [33]. 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 [44], where each shard is responsible for computing a subset of the overall transactions. 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 heterogeneous blockchains, we need to use cross-chain communication, a set of techniques allowing us to share data and transfer assets between blockchains, by relying on parties external to the involved blockchains. This concept seems prone to security vulnerabilities, and it is indeed - around $3B in losses happened only in blockchain bridges, the most popular cross-chain applications [4, 11] (there are more than 110 bridges[1] with a capitalization of almost 18B USD as of December 2023[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 [33, 46].

## 2 DECONSTRUCTING INTEROPERABILITY MECHANISMS - THE PRESENT

Since 2016, when the interoperability research area started attracting attention, its focus has shifted. Many systematizations of knowledge appeared from 2016 to 2021 (namely 11), highlighting new categories of solutions: sidechains (2015/2016), blockchain-of-blockchains (2016/2017), relays (2019), blockchain agnostic protocols (2019/2020), solutions for the enterprise (2019/2020), and even preliminary techniques for blockchain migration (2020). Since then, the focus has been on generalization, standardization, and refinement of existing techniques (see [9]). A visible trend is on orchestrating arbitrary logic spanning across centralized and decentralized infrastructure to realize the following 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 [36] 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[3]. 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

[1]https://chainspot.io/
[2]https://l2beat.com/scaling/summary
[3]https://docs.blockdaemon.com/reference/

surface is very large [4, 49]. Finally, *asset exchanges* consist of 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, which are mediated by off-chain processes and smart contracts.

Many of these advances were made possible due to the (recent) standardization effort of data formats (e.g., view [13]) and token interfaces (e.g., ERC-721, xERC20, ERC-6358), protocols, and blockchain IDs[4].

### 2.1 A Look at the Industry

To understand the current interoperability landscape, note that the market has over 100 solutions today [19]. 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, which specialize in one task. We hypothesize that teams are increasing their focus on GMP protocols (e.g., [7]), popularized in 2021/2022, because the expressiveness of the data they can handle allows for developing flexible solutions, by leveraging data transfers as the basis for asset transfers. 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 1 illustrates.

While compared to more limited solutions, the development of generalized messaging protocols is more laborious. However, 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 bridge aggregator Squid Router; liquidity network Stargate and Aptos Bridge, both built on top of LayerZero (see the full version for technical details [12]) as 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 bridge's security is directly pegged to the underlying (source) blockchain. Extensibility means the bridge can support additional blockchains without major refactoring. Generalizability means the bridge can perform both data 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 different categories (refer to the full version of this paper for a description [12]).

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 [4, 11, 41]. 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

[4]https://chainlist.org/

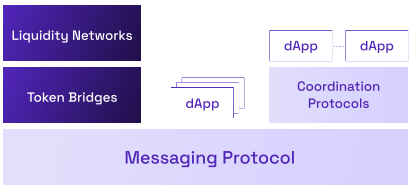


Fig. 1. Layers of cross-chain communication protocols [1]

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, a new approach to trust in interoperability is to look at it as a spectrum.

## 2.2 Current obstacles and challenges

There are many ongoing challenges in interoperability, many of which are systematized in [9, 15, 32] and still remain up-to-date. According to the authors' recent research, the problems we believe are the most prominent as of February 2024 are security monitoring [5, 11], systematic benchmark of interoperability solutions [10, 43], and privacy [5]. An orthogonal problem in the area is the lack of uniformization of terms and vocabulary: the academia and industry sometimes speak different languages in this research area, in particular on rollups research.

*2.2.1 Cross-chain privacy.* It is generally agreed upon that anonymity (in terms of unlinkability), confidentiality, and indistinguishability of transactions are beneficial privacy properties in the cross-chain context [4, 47]. 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 [42], 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 [22]. Privacy on asset exchanges looks more straightforward than other interoperability modes: HTLCs share secrets only understandable by the involved parties, making it 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. Recent work has revealed interesting insights on cross-chain privacy [4], namely its de-prioritization compared to security, common usage of zero-knowledge proofs, current high latency and transaction cost overheads, the need to educate end-users, and that full privacy is only attainable if the underlying ledger provides privacy features.

*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]) and a few interoperability solutions are assessed in detail [20]. 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 [8]), 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. A good starting point is directed to evaluate scalability (in terms of the number of blockchains and tokens supported) cross-chain latency, throughput, and transaction costs on popular bridges. There is industry interest in studying 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. 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, 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 [23]. 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 [11]could be interesting directions for future work.

## 3 THE FUTURE OF BLOCKCHAIN INTEROPERABILITY

What trends will we assist in the next few years? To answer this question, there are some trade-offs to consider, namely the mentioned interoperability trilemma tradeoffs: trustlessness, extensibility and generalizability. As the industry seems to have prioritized the last two tradeoffs, it is not surprising that the trends reflect an evolution in this sense.

The first trend is the usage of a modular stack design, and hence the emergence of cross-chain applications. 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 applications that coordinate dependent transactions across two or more networks such as cross-chain *decentralized exchanges* (DEXs), also called DEX aggregators. Sushiwap and

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

Stargate Finance on LayerZero, Squid Router on Axelar, and Osmosis on IBC are examples of cross-chain DEXes enabled by different interoperability solutions. More use cases considered by the IETF are documented here [40]. Those reflect the need of integrating blockchains with centralized systems in the areas of supply chain (transfers of letters of credit, also reported here [13]), currency transfers across central bank digital currencies (also reported here [6]), delivery vs payment (DvP) of securities, and transfer of digital art across jurisdictions.

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[16]. 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[31] or SNARKs [8]. This is related to the emergence of bridge aggregators, software systems that expose several existing bridges in a single interface. Such interface 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 [11]. The end user would be able to choose from a range of options depending on their specific needs, availability of liquidity, and connectivity. The trend is analogous to infrastructure providers such as Blockdaemon taking on the complexity of managing the analysis, deployment, and maintenance of hundreds of different blockchain protocols on behalf of their clients.

The third trend is the potential consolidation of GMPs similar to the consolidation in Layer 1 networks (see for example [24]), 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.

## 4 KEY TAKEAWAYS

Recent developments in blockchain have been incredibly exciting, unveiling a realm of possibilities that were not possible three 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 other decentralized and centralized systems, which are not going to be replaced. 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 supported by the European Commission under project BIG ERA Chair (grant agreement 952226) and 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).

## 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] Al-Breiki, H., Rehman, M. H. U., Salah, K., and Svetinovic, D. Trustworthy blockchain oracles: review, comparison, and open research challenges. *IEEE access 8* (2020), 85675–85685.

[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] Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., and Hardjono, T. Sok: Security and privacy of blockchain interoperability. TechRxiv Preprint, 2023. Online; accessed on December 22, 2023.

[5] Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., and Hardjono, T. Sok: Security and privacy of blockchain interoperability, 2023. Preprint accessed on 22 December 2023.

[6] Augusto, A., Belchior, R., Vasconcelos, A., Kocsis, I., László, G., and Correia, M. Cbdc bridging between hyperledger fabric and permissioned evm-based blockchains. TechRxiv Preprint, 2023. Online; accessed on December 22, 2023.

[7] 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.

[8] Belchior, R., Dimov, D., Karadjov, Z., Pfannschmidt, J., Vasconcelos, A., and Correia, M. Harmonia: Securing cross-chain applications using zero-knowledge proofs. https://rafaelapb.github.io//harmonia, 2023. Online; accessed on December 22, 2023.

[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., Scuri, S., Mihaiu, I., Nunes, N., and Hardjono, T. Towards a common standard framework for blockchain interoperability - a position paper, Oct. 2023. Citation Key: belchiorCommonStandardFramework2023a.

[11] Belchior, R., Somogyvari, P., Pfannschmidt, J., Vasconcelos, A., and Correia, M. Hephaestus: Modeling, analysis, and performance evaluation of cross-chain transactions. *IEEE Transactions on Reliability* (2023), 1–15. Citation Key: belchiorHephaestusModelingAnalysis2023.

[12] Belchior, R., Süssenguth, J., Feng, Q., Hardjono, T., Vasconcelos, A., and Correia, M. A brief history of blockchain interoperability. TechRxiv Preprint, 2023. Online; accessed on December 22, 2023. Full version of current paper.

[13] Belchior, R., Torres, L., Pfannschmid, J., Vasconcelos, A., and Correia, M. Can we share the same perspective? blockchain interoperability with views. TechRxiv Preprint, 2023. Online; accessed on December 22, 2023.

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

[15] 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.

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

[17] Buterin, V. Chain interoperability. *R3 Research Paper 9* (2016), 1–25. Accessed December 22, 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] Chainspot. Find your bridge with the largest blockchain bridges aggregator, 2021. Available online: https://chainspot.io/, last accessed on 2023-05-21.

[20] 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).

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

[22] 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.

[23] 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.

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

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

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

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

[28] 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.

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

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

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

[32] Jin, H., and Xiao, J. Towards trustworthy blockchain systems in the era of "internet of value": development, challenges, and future trends. *Science China Information Sciences 65* (2022), 1–11.

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

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

[35] Lerner, S. P2ptradex: P2p trading between cryptocurrencies. https://bitcointalk.org/index.php?topic=91843.0, 2012. Online; accessed on December 22, 2023.

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

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

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

[39] Nolan, T. T. Re: Alt chains and atomic transfers. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949, 2013. Online; accessed on December 22, 2023.

[40] Ramakrishna, V., and Hardjono, T. Secure asset transfer (sat) use cases. Internet-draft, Internet Engineering Task Force (IETF), 7 2023. Working Group: satp. Draft version: draft-ietf-satp-usecases-01. Replaces: draft-ramakrishna-sat-use-cases.

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

[42] 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.

[43] Subramanian, S., Augusto, A., and Belchior, R. Benchmarking bridge aggregators, Jan. 2024. Citation Key: subramanianBenchmarkingBridgeAggregators2024.

[44] 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.

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

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

[47] 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.

[48] 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.

[49] 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).