EUBlockchain
Observatory and Forum

The current state of interoperability between blockchain networks

About this report

This is the second of a series of reports that will be published addressing selected topics in accordance with European Commission priorities. The aim is to reflect on the latest trends and developments and discuss the future of blockchain in Europe and globally.

This report has been produced by the EU Blockchain Observatory and Forum Experts Panel and team.

The EU Blockchain Observatory and Forum team:

- Nikolaos Kostopoulos, Konstantinos Sekaras, Nicolas Sarafidis, Ioannis Vlachogeorgakopoulos Netcompany-Intrasoft
- Alexi Anania, EUBOF Expert Panel
- Wendy Charles, EUBOF Expert Panel
- Catarina Ferreira da Silva, Instituto Universitário de Lisboa, ISCTE-IUL, ISTAR
- Amit Joshi, HashPrix
- Urko Larrañaga, EUBOF Expert Panel
- Jim Mason, The Depository Trust & Clearing Corporation (DTCC)
- Inigo More, EUBOF Expert Panel
- Daniel Szego, EUBOF Expert Panel
- Ingrid Vasiliu-Feltes, University of Miami

Note

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this report.

Disclaimer

CHAPTER 1 UNDERSTANDING THE CONCEPT OF BLOCKCHAIN INTEROPERABILITY

1.1 WHAT IS BLOCKCHAIN INTEROPERABILITY

Blockchains have attracted significant attention due to their potential to revolutionise industries. However, improvements in the area must be made for the ecosystem to scale.

Traditionally, blockchain networks run individually, each resolving a particular issue, making the field fragmented and compromising its scalability. This may lead to risks of security breaches due to potentially more bugs and a smaller user base (Schulte-Merker, S., Sigwart, M., Frauenthaler, P., & Borkowski, M. (2019)).

However, to make their adoption widespread and to fully take advantage of the technology, it is crucial to 'provide interoperability between blockchains in order to explore synergies between different solutions, scale the existing ones and create new use cases' (Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021)).

Blockchain interoperability, referred to as '**the ability of blockchain networks to communicate with each other, sending and receiving messages, data, and tokens'** (Chainlink. (2023)) is therefore emerging as a requirement for the continuity of blockchain technology. Indeed, it will enhance productivity throughout the whole crypto sector because users can quickly move data and assets, which increases flexibility (Clarke, A. (2022)).

However, due to the complexity, there are some challenges that need to be tackled. Indeed, each blockchain system varies from another due to its governance model, speed of confirmation, strength of consensus, degrees of permissibility, degree of anonymity, and the cybersecurity and assurance levels of the nodes (T. Hardjono, A. Lipton and A. Pentland (2020)) making the coordination between networks complex and challenging to standardise.

This report discusses the potential of blockchain interoperability and its challenges.

The blockchain was not designed with built-in interoperability capabilities, a challenge that emerged only when users defined specific needs for connections. The success of blockchain technology produced the emergence of many chains, creating a general use case for interoperability. In fact, it could be also considered a necessity, as otherwise any investment or asset in a blockchain will be subject to unbearable risks such as potential vendor lock-in. From this point of view, interoperability is also a condition for further development of the user base of this technology.

Blockchain interoperability is a problem that emerged, with written references, in 2014. Then, somebody under the username u/dalovindj posted a comment on Reddit's Bitcoin thread about an issue that he called 'The oracle problem'. At the time, 'block chain', was still written as two separate words[1], while Ethereum did not exist except in the mind of Vitalik Buterin, still working as a journalist on a magazine devoted to Bitcoin.

---

[1] [1] Satoshi never use the word "blockchain" in his whitepaper where expressions such as "chain of blocks" can be found. Hal Finney was the first person on record to use the two words "block chain" in November 2008 as it can be seen in the Cryptography Mailing List in a conversation with Satoshi https://satoshi.nakamotoinstitute.org/emails/cryptography/6.. The two words formula evolved later into the actual blockchain.

In this early moment of blockchain technology, the issue raised by the Reddit user (u/dalovindj) was related to several use cases of Bitcoin, one of which was prediction markets. Assuming that somebody placed a prediction on a baseball match, his question was, 'How does a system determine that the Red Sox won last night?' Traditional systems solve this problem by connecting with trusted sources, for instance, the Major League, that act as an oracle. In classical Greece, oracles were people who had the ability to communicate with a deity, allowing them to supply wise opinions, even foresee the future. Regarding blockchain, U/dalovindj wondered 'how to produce trusted oracles (sources of determinations of the outcomes of conditions)'. At the time, nobody had a solution, but u/dalovindj defined a problem related to Bitcoin's blockchain structure: it was not designed to communicate with other blockchains (because no other one existed when launched) and nor with any other external source. This lack of built-in communication capability prevented any immediate connection. Back in 2014, this was seen as an issue affecting interaction between blockchain and traditional systems. But today we have a blockchain rich environment, with many independent networks that usually operate in isolation, preventing the exchange of data and assets between them. It is a fragmented ecosystem where the oracle problem is understood in relation to the interoperability between blockchains. The difficulties in achieving interoperability between blockchains lie in their internal structure, which may be based on different consensus mechanisms, protocols, rules, or features. Interoperability refers to mechanisms and strategies that overcome these barriers and allow interaction, including the transfer of data or assets across blockchains. Its most generalised use case today could be identity verification, which may involve additional issues in a heavily regulated field, from data protection to potential forgeries.

Achieving interoperability

Blockchain interoperability is a challenge that only became evident six years after the launch of Bitcoin. However, it took much longer to be generally recognised as a limitation, not only for technological reasons, but also because of the development of the market. In 2016, Vitalik Buterin recognised that 'the notion of chain interoperability has seen much theory and little practice'. In his opinion, this was due to the fact that a 'successful chain interoperability requires not one, but two, already existing, stable and sufficiently powerful blockchains' (Chain interoperability- R3 Research Paper (2016).

There are many tools that could facilitate blockchain interoperability (see the section below on 'Approaches to Interoperability'), allowing them to exchange information and also share it. This lies in the use of tools that add new capabilities, in the same way that new mechanisms can be retrofitted into an existing machine. The choice between one or the other would rely on the desired outcome, level of security, or the specific aspects of the chains meant to interoperate.

1.2 THE IMPORTANCE OF BLOCKCHAIN INTEROPERABILITY

Since its inception, and as a relatively nascent technology, blockchain has emerged as a transformative force, heralding an era of decentralised systems that aspire to revolutionise infrastructural sectors as diverse as finance, the supply chain, and more. However, while the prospect of a blockchain-empowered future is enticing, it is contingent on continuing to address a key challenge: interoperability. The capacity for diverse blockchain systems to interact and exchange information is pivotal to harnessing blockchain's full potential, while addressing key benefits and eliminating drawbacks.

The current blockchain ecosystem consists of an array of distributed ledgers, each functioning within their isolated silos. Currently, there are thousands of blockchain networks in existence. These include Bitcoin, Ethereum, Cardano, Ripple, and countless others, each with unique protocols, consensus mechanisms, and cryptographic algorithms. Without interoperability, these blockchain networks remain isolated, limiting their effectiveness, reach, and scope.

Blockchain interoperability involves the ability of different blockchain networks to communicate with each other, exchange data, and conduct transactions seamlessly. This integration facilitates the smooth transfer of any type of data or asset from one blockchain network to another. The importance of blockchain interoperability lies in its capacity to link together an increasingly fragmented blockchain ecosystem and harness the unique advantages of each separate chain.

Inherent in the promise of blockchain is the concept of decentralisation. This concept encompasses a move away from centralised authorities that possess singular control, towards distributed systems where control and trust are disseminated amongst many nodes. By design, blockchains are intended to create systems that are transparent, secure, and immutable, where any participant can verify transactions (Nakamoto, 2008). However, without interoperability, we may inadvertently end up with a new form of centralisation, where certain blockchain ecosystems dominate at the expense of others. Blockchain interoperability is therefore essential in maintaining the core ethos of decentralisation.

Interoperability is also crucial for broader blockchain adoption. As diverse industries adopt blockchain technologies, they will inevitably require systems that can exchange and validate information across different chains. As an example, a logistics company using one blockchain might need to validate transactions with a financial institution using another. If these systems cannot interoperate, blockchain's potential for a viable global commercial use case is still out of reach.

In addition to unifying the blockchain ecosystem, interoperability also promotes innovation. By enabling communication and data sharing between distinct blockchain platforms, developers are provided with a broader canvas on which to paint their solutions. Without interoperability, there is a risk of creating isolated 'innovation islands', where progress in one chain does not benefit the broader ecosystem (Wang et al, 2017). By enabling cross-chain communication, we can encourage a more collaborative and innovative environment. Developers can leverage the unique strengths of different blockchains to build hybrid applications that are more versatile, robust, and efficient.

Interoperability also fosters inclusivity in the blockchain ecosystem. It allows for a diversified and democratic digital environment where all blockchains, regardless of their size or user base, have the potential to contribute to the global value chain. This inclusivity not only encourages the innovation of diverse solutions, but also a more robust and resilient blockchain ecosystem.

Another noteworthy benefit of interoperability is enhanced security. The current lack of interoperability often forces users to store their assets on multiple platforms, each with its own security assumptions and vulnerabilities. This situation exposes users to higher risk levels. Interoperability can streamline asset management by allowing users to manage and move their assets across various chains securely and efficiently. While this exposes a larger surface area for vulnerabilities, once addressed and as an end objective it would be safer and less complicated from a user perspective.

Several initiatives discussed in this paper are currently underway to address the challenge of blockchain interoperability. Yet it is important to acknowledge that, while the indispensable role of blockchain interoperability is evident, blockchain interoperability is not without challenges. Technical complexities, intrinsic security concerns from modularity, and the need to maintain decentralisation while fostering interoperability all pose considerable obstacles. These complexities include:

1. ensuring transaction finality across different chains;
2. managing cross-chain smart contract execution; and
3. maintaining data integrity during cross-chain communication.

Furthermore, given the nascent nature of the technology, regulatory and legal frameworks around cross-chain interactions are still evolving.

The importance of blockchain interoperability cannot be overstated. It serves as a conduit for unlocking the true potential of blockchain by bridging these digital islands. Interoperability allows the movement of assets and data between different chains, enabling a fluid and integrated blockchain ecosystem that offers the best of every chain. This fluidity is especially crucial in applications such as decentralised finance (DeFi), where seamless value transfer and interaction across multiple blockchains can significantly fill liquidity fragmentation gaps and create more robust financial products.

Interoperability is integral to ensuring the decentralisation ethos of blockchain, crucial for broader adoption across diverse industries, and vital for fostering a collaborative and vibrant innovation environment. While there are significant challenges to be addressed, the ongoing development of cross-chain protocols, bridges and blockchain standards are promising steps towards a more interconnected blockchain future.

1.3 APPROACHES TO INTEROPERABILITY

Blockchain technology has gained widespread adoption because it provides a secure, decentralised platform for transactions, data storage, and smart contracts. However, despite significant progress, blockchain interoperability remains a persistent challenge in the blockchain industry (Kotey et al., Wiley, 2023).

In this chapter, we will examine the challenges we must overcome, and the opportunities offered by enhanced blockchain interoperability. We will highlight the future of blockchain interoperability from a technological perspective and its impact on the business ecosystem. The influence and value proposition of blockchain interoperability transcends industries. Therefore, we will focus on several high-impact domains, such as their role in transitioning to the next generation of the world wide web (Web 3.0 and beyond), the development of smart global ecosystems, and the creation of new ecosystems (for example, creator economy, net zero economy, metaverse, and omniverse-economy).

1.3.1. Cross-Chain Interoperability

Cross-chain interoperability pertains to creating protocols, technologies, and standards that enable the transfer of digital assets between different blockchains without centralised exchanges or intermediaries (Khan et al., 2021). A cross-chain transaction is a transaction between chains belonging to the same blockchain system, while a cross-blockchain transaction is a transaction between different blockchains.

Cross-chain interoperability creates benefit by offering novel opportunities for decentralised applications (DApps) to engage with diverse blockchain platforms. However, the premise of secure cross-chain interoperability is based on the assumption that the mainchain is impervious to security breaches that would nullify sidechain logic (Belchior et al., 2022).

1.3.2. Protocol Interoperability

Blockchain networks frequently use distinct protocols that incorporate varying consensus mechanisms, data structures, and transaction formats. Protocol interoperability offers capabilities for different blockchains to achieve compatible protocols. The process requires developing standard protocols and interfaces for communication among various blockchain systems.

A cross-chain communication protocol (CCCP) is a standard protocol to facilitate synchronisation between two homogenous chains (Wang, Wang, & Chen, 2023). For example, Belchior et al. (2022) note that it is possible for two similar blockchain systems (such as two Bitcoin blockchains) to use CCCPs as an effective method to interoperate. In contrast, a cross-blockchain communication protocol (CBCP) delineates how heterogenous blockchains synchronise transactions (Belchior et al., 2022). For example, the Interledger Protocol facilitates the exchange of 'money packets' among blockchains with different platforms that have implemented the Interledger Protocol (Interledger.org, 2023).

Unfortunately, designing a cross-chain communication protocol presents a challenge due to the potential deployment of varying consensus protocols, block sizes, confirmation times, hashing algorithms, or network models across different blockchains (Wang, Wang, and Chen, 2023). Additionally, it is difficult to detect and verify data recorded on one chain solely by observing exchanged information from another chain. According to Wang, Wang, and Chen (2023), the transfer of assets can be facilitated by the involvement of a trusted centralised intermediary. However, including a trusted intermediary seems to violate one of the fundamental tenets of blockchain technology: decentralisation (Wang, Wang, and Chen, 2023).

1.3.3. Data Interoperability

Data interoperability entails the creation of protocols, data models, and data mapping mechanisms that facilitate the seamless exchange of data across disparate blockchain networks. The concept of ‘data’ could include credentials and operational data stored on the blockchain or index and raw data stored off-chain (Abebe et al., 2019).

However, differences in data formatting, storage, and endorsement across various blockchain platforms has resulted in the inability of voucher data and deposit certificates to be recognised in different systems (Zhu, Chi, and Liu, 2023). In contrast to the substantial volume of data that can typically be accommodated in conventional data-sharing systems, the data housed within blockchain systems must be validated by the blockchain itself (Zhu, Chi, and Liu, 2023).

1.3.4. Asset Interoperability

The rapid growth of Bitcoin has led to the creation of thousands of cryptocurrencies and crypto assets stored on a wide variety of blockchains (Zhang et al., 2022). The presence of heterogeneous and siloed assets created a marked need for asset interoperability and exchange. Asset interoperability enables the transfer of various assets such as tokens, cryptocurrencies, and crypto assets such as non-fungible tokens (NFTs) (Belchior et al., 2022). Asset interoperability plays a crucial role in improving the fungibility and market penetration of digital assets, thereby promoting wider acceptance.

Asset interoperability requires the ongoing development and refinement of protocols, bridges, and/or token standards that enable the smooth transfer and compatibility of assets across diverse blockchain networks. According to Zhang et al. (2022), cross-chain bridges have emerged as a prominent approach for enabling asset interoperability. However, while there is great potential for effective and adaptable cross-chain asset transfer, the complex workflow between on-chain smart contracts and off-chain programs creates security vulnerabilities.

1.3.5. Smart Contract Interoperability

Smart contracts refer to autonomous computer programmes designed to execute, validate, or enforce contractual terms without human intervention. Smart contracts are commonly associated with a particular blockchain network and are written in many different programming languages.

Smart contract interoperability aims to streamline the implementation and engagement of smart contracts across various blockchain networks. According to Khan et al. (2021), smart contract interoperability entails expanding a contract written in a particular programming language to other blockchain networks by referencing their specific contract code. The process requires creation of established protocols, standards, and/or bridges that facilitate the execution of smart contracts across multiple chains and the ability to operate in conjunction with one another. As an example, Khan et al. (2021) note that a virtualisation-based strategy facilitates the implementation of a smart contract on heterogenous blockchain platforms by establishing an abstraction layer over the primary blockchain. There are current initiatives to design user interface-based engines that can facilitate the generation of intelligent contract workflows across multiple blockchains (Khan et al., 2021).

1.4 CHALLENGES APPLYING BLOCKCHAIN INTEROPERABILITY

1.4.1 TECHNICAL CHALLENGES

A recent paper (Gang Wang et al., ACM Journal, 2023) emphasises why integrating heterogeneous and homogeneous distributed ledgers in the next generation blockchain ecosystem poses significant challenges for ensuring seamless operations across multiple blockchains. The authors also highlight that further development of blockchain interoperability requires tackling the complexities arising from diverse underlying architectures to guarantee ACID (atomicity, consistency, isolation, durability) properties. Distributed and decentralised storage systems cannot guarantee ACID properties. However, they can follow the Brewer theorem or CAP (consistency, availability, partition tolerance) theorem. As the adoption of blockchain technology increases and blockchain interoperability evolves, so will the need for proactive, state-of-the-art digital ethics and cyber resilience programs. These will be crucial to managing the next generation of blockchains and mitigating the increased risks of data breaches possible with increased blockchain interoperability.

1.4.2 CYBER ETHICS

The convergence of different technologies, including blockchain, digital twin technologies, and quantum computing, has created new opportunities for data exchange and value creation. However, it has also created new risks, including cyber-attacks, data breaches, and ethical dilemmas. As more networks become interconnected, the potential for vulnerabilities increases and the need for robust cyber resilience and digital ethics programs becomes paramount.

In another paper published (Trivedi et al., Wiley 2023), the authors demonstrate how in recent years Internet-of-Things (IoT) applications have shifted their focus from centralised to decentralised infrastructures, primarily due to security and privacy concerns over user data. However, this shift has also increased vulnerability to distributed attacks in diverse IoT scenarios, jeopardising the application environments. To address these limitations, the authors highlight that blockchain-based IoT systems and platforms could be the solution, ensuring data consistency, immutability, and chronology in IoT environments.

Conversely, experts have called attention to the increased risks of data breaches associated with increased blockchain interoperability. Blockchain technologies are known for enhanced security features, including decentralised data storage, encryption, and immutability. However, when different blockchains communicate and share information, the potential for data breaches increases. In addition, cybercriminals may exploit vulnerabilities in one blockchain to access another, compromising security and integrity.

Proactive digital ethics and cyber resilience programmes are needed to mitigate the risks associated with increased blockchain interoperability. These programmes must address the ethical dilemmas associated with data exchange and value creation and the technical challenges of securing interconnected networks.

Digital ethics programmes should guide the responsible use of blockchain technology, including data privacy, consent, transparency, and accountability. In addition, they should address the ethical implications of blockchain interoperability, including the potential for unintended consequences and the need to balance innovation with social responsibility.

Cyber resilience programmes should provide technical solutions to mitigate the risks of data breaches and cyber-attacks. These programmes should include measures to identify vulnerabilities, monitor network activity, and respond to real-time security incidents. They should also include disaster recovery plans and business continuity plans to minimise the impact of security incidents on business operations.

As we continue to move from perimeter cybersecurity toward zero trust principles, near real-time scrutiny of lateral movements involving users, devices, and services within the networks are required. Blockchain technologies and architectures offer a solid opportunity to implement such zero trust capabilities, even in the face of legacy and other heterogeneous systems. We are looking forward to advancing research, innovation, and applications of these emerging technologies to improve security controls for the many systems that process sensitive data'. said Steve Dennis, visiting fellow, Institute for Data Science and Computing, University of Miami.

Proactive digital ethics and cyber resilience programmes should be integrated into the design and development of blockchains. Security and ethical considerations should be integral to the blockchain development lifecycle, from requirements gathering to testing and deployment. This approach ensures that security and ethical considerations are discussed early in the blockchain assessment and deployed early in the design phase.

1.4.3 STANDARDS, METRICS, and KPIs

In addition to proactive digital ethics and cyber resilience programmes, blockchain interoperability requires the development of robust international interoperability standards, metrics, and key performance indicators (KPIs). These standards and metrics should cover technical, ethical, regulatory, and legal considerations, providing a comprehensive framework for interoperability.

Anybody building a blockchain today would devote efforts to addressing this issue of interoperability from the beginning. Success would be easier thanks to the efforts to standardise blockchain, and, in particular, its interoperability. One example of these efforts comes from the European Telecommunication Standards Institute, which produced a technical document on inter-ledger interoperability developing common standards for protocols or data formats, allowing compatibility, and facilitating interoperability across different blockchains. One simple aspect of the document is the definition of ‘standard fields for interoperability’ which include the distributed ledger identifier, the node identifier or the shareable data fields. Just by adhering to a standard, the interoperability capabilities of any new blockchain will be greatly enhanced. And this will be the straightest route to the gold standard of the field, ‘seamless interoperability’, as the security, speed, reliability, or ease of implementation of every solution differ vastly. This role of institutions is likely to increase in the future, as demonstrated by other technologies that faced the same problems some time ago. One example is the telephone, whose international connectivity would not be the same without UN agencies such as the International Telecommunication Union.

CHAPTER 2 TYPES OF CROSS-CHAIN INTEROPERABILITY SOLUTIONS

Several types of blockchain interoperability aim to facilitate communication and data exchange between different blockchain platforms. However, there is no agreement about the types of blockchain interoperability. Therefore, in the absence of a clear consensus on blockchain interoperability classifications, this report has classified blockchain interoperability methods into the following categories for convenience: 1) public connectors - side chains and chain relays, notary schemes, 2) atomic swap protocols & cross-chain automated market makers, and 3) application-specific blockchains.

2.1 PUBLIC CONNECTORS

2.1.1. Side Chains and Chain Relays

A sidechain is a kind of blockchain connected to another primary blockchain, known as the mainchain. This connection allows assets to move between multiple blockchains. Sidechains are isolated, meaning that if something goes wrong on a sidechain, it does not affect the mainchain. To transfer assets from the mainchain to the sidechain, sidechains first lock the assets on the mainchain.

The transfer process follows these steps.

1. A user sends an asset from the mainchain to the sidechain, where it is temporarily locked.
2. The sidechain automatically allocates the deposited funds with the user.
3. The user can now use these funds on the sidechain, often at lower transaction costs.
4. Periodically, a checkpoint of the latest blocks from the sidechain is sent to the mainchain, ensuring security.
5. Finally, the user can get their funds back from the mainchain anytime. There is a delay to prevent disputes and double spending. This delay is necessary because sidechains work on fraud proofs, which let users prove invalid transactions.

Relay chains are more complex, combining features of notary and side chain frameworks. They use light-client verification technology to connect different chains and facilitate cross-chain communication. Relay chains have practical applications like cross-chain asset exchange and contract implementation.

Side chains are easy to implement, have various uses, and enhance blockchain interaction. They also increase the mainchain's scalability. However, side chains add complexity to the network and can introduce new attack risks. Finally, they do not completely solve interoperability issues as they still rely on trust.

2.1.2. Notary Schemes

A notary is a trusted entity which manages multiple chains and initiates transactions on the basis of certain events, usually using smart contracts. Notary schemes act as intermediaries between blockchains.

Notary schemes use a trusted middleman to oversee transfers between parties who mistrust each other. However, this approach can often lead to centralisation. For instance, decentralised exchanges act like notaries by matching end-users through trade offers coded in smart contracts.

Notary schemes are easy to implement and can support different blockchain networks. They also distribute trust to the notaries and provide flexibility. However, they can reduce decentralisation and become a single point of failure, meaning if the notary fails, the whole system could go down.

2.2 ATOMIC SWAP PROTOCOLS & CROSS-CHAIN AUTOMATED MARKET MAKERS

Cross-chain atomic swaps and cross-chain automated market makers create a kind of communication between different blockchain systems. While atomic swaps and cross-chain tokens deal more with the technical side of integrating different blockchain platforms, cross-chain market making helps to create a fluid token market between tokens produced by different blockchains. Let's dive a bit deeper into these topics.

Cross-chain atomic swap

A cross-chain atomic swap is like a link that joins two blockchains for transactions. It ensures that a transaction on one blockchain happens only if a transaction on another blockchain happens too. In simple terms, either both transactions occur, or none occur at all.

For example, if you want to exchange Bitcoin for Ether, Bitcoin's transfer happens on the Bitcoin blockchain while Ether's transfer happens on the Ethereum platform. The goal here is that both the Bitcoin and Ether transfers occur together. Either both Bitcoin and Ether get transferred, or none get transferred. Plus, in line with the blockchain philosophy, this process should be as decentralized as possible, avoiding the need for a trusted third party.

Atomic swaps make trading easier on the blockchains involved by using something called hash-locks and time-locks. This means that no third-party is needed (Bishnoi and Bhatia, 2020). These hash-lock and time-lock mechanisms make the person receiving the transaction confirm payment by providing cryptographic proof within a certain time (Bishnoi and Bhatia, 2020).

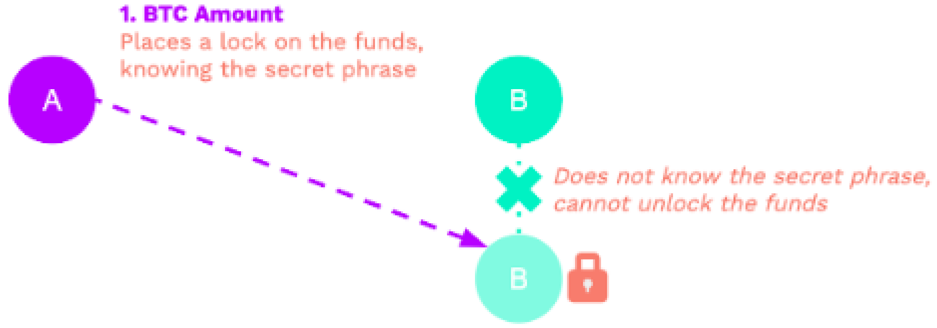

Figure 1: Hashed timelock contract

Hash-locking is used to move assets without needing a trusted middleman. It involves a system called a hash time-locked mechanism, which sets a time limit for securing transactions. Until both parties involved have agreed on their responsibilities, the transaction remains locked.

Once agreed, the parties unlock the assets that are held in smart contracts on different chains. They do this by sending hash proxies and hash values and setting their time locks to allow for atomic operations, which are all-or-nothing operations. This process either speeds up the transaction or makes it fail. Hash-locking ensures the total assets in a chain are kept safe.

The atomic swap protocol uses something called a hashed time lock contract (HTLC) when exchanging assets. This allows temporary control over the other party's assets. A user in an HTLC must provide cryptographic proof to complete a transaction before a set time limit. If they do not provide the key within that time, the assets stay with the original owner.

HTLC is often used within payment channel networks (PCNs), which are private channels where parties can update states by trading off-chain authenticated state transitions. Using HTLC in PCNs is a good alternative to setting up payment channels and helps maintain good transaction speed.

The atomic cross-chain swap is the foundation for many general interoperability solutions like Hyperledger Cactus or integrated wallet token swap services.

The benefits of hash-locking include secure and seamless asset transformation between Ethereum and other blockchain networks. It provides atomicity (all-or-nothing transactions), fairness, and transparency.

However, hash-locking is not a perfect solution. Assets can get lost due to the timeout, and dishonest participants can issue fake transactions. Setting up multiple transactions is also complex. There is also a time delay in asset transfer, which can be unfair as the initiator of the transaction has the power to decide whether to trade or not. Lastly, hash-locking is suitable for asset exchange but not asset transfer, limiting its usefulness.

Cross-chain tokens

A cross-chain token is another method to technically integrate two blockchains. Most DeFi (decentralised finance) solutions are built on a specific blockchain, like Ethereum, but sometimes there is a need to use tokens from another blockchain. For example, you might need to use bitcoin within the Ethereum ecosystem.

Cross-chain tokens provide a solution by mirroring a token from one blockchain onto another, while ensuring that double-spending across chains is not possible. This means you can either spend the original token on its native blockchain or the mirrored token on the other blockchain, but not both.

Here is a simplified explanation of how cross-chain tokenisation, such as replicating bitcoin on the Ethereum network, works:

Issuance: This is the process of creating a mirrored token on another network. In our example, we want to mirror bitcoin onto the Ethereum network.

To bring bitcoin into the Ethereum ecosystem, the bitcoin must first be conditionally locked on the Bitcoin blockchain. This means the bitcoin cannot be spent on its original network. The locking mechanism is usually achieved through methods similar to HTLCs (hashed timelock contracts) that we previously discussed.

On the Ethereum network, a new token is issued, commonly referred to as a 'wrapped' token, like wrapped bitcoin (wBTC). This token represents one bitcoin within the Ethereum ecosystem.

It is important to ensure that the token on the original network is truly locked and can only be unlocked under certain conditions during issuance. The flow of information between the two networks is often decentralised through the use of decentralised oracle platforms. These platforms verify that the conditions on the original network have been met before allowing the issuance of the mirrored token on the second network.

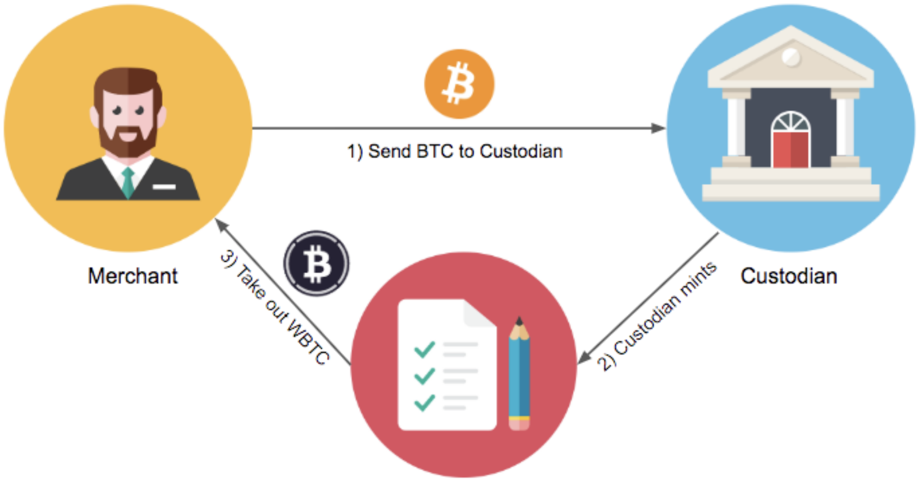

Figure 2: Wrapped Bitcoin

Redemption is the process of converting the mirrored token back into the original token. This process involves the following.

Burning the wrapped token on the target network: This is the process of permanently removing the mirrored token from the blockchain's supply. In our previous example, this would mean burning wrapped bitcoin (wBTC) on the Ethereum network.

Unlocking the token on the original network: After the wrapped token is burned, the corresponding amount of the original token is unlocked on its native blockchain. In this case, BTC would be unlocked on the Bitcoin network. It is crucial to ensure a reliable and as decentralised as possible flow of information between the two networks during this process.

Cross-chain tokens are often key components of more complex bridging solutions like Hyperledger Cacti and wBTC.

Cross-chain automated market makers (AMMs) integrate blockchains more from a business perspective, focusing on tokens and liquidity. Essentially, a liquidity pool-based decentralised exchange holds pairs of tokens in smart contracts. Traders do not trade directly with each other but interact with the smart contracts. The token prices are determined automatically by an automated market making algorithm.

The most commonly used pricing mechanism is the **constant product market maker (CPMM)** algorithm. It uses the formula x*y=k, which sets a range of prices for two tokens based on their available quantities (liquidity).

One advantage of AMM pricing mechanisms is that they operate fully on-chain. However, they also have several disadvantages. For example, they might not reflect the market price in the short term. While it is assumed that traders will actively exploit arbitrage opportunities between different markets – ensuring that the AMM's pricing aligns with the broader market – this isn't always the case.

Furthermore, providing liquidity for an AMM can lead to unexpected costs, known as **impermanent loss**. This happens when the market prices of tokens in a liquidity pool change compared to when they were deposited, resulting in less value when the liquidity is withdrawn.

There can also be issues when trading certain type of tokens with specific AMM formulas. For instance, stablecoins, whose prices are strongly correlated with each other, can present unique challenges.

Cross-chain automated market making tries to extend the original AMM and liquidity pool-based DEX concept from a one chain model to a multiple chain solution. The first version liquidity pool-based DEX-s were built solely on one chain, effectively limiting the possible tokens that can be provided and traded by liquidity pools. One way of extending the one chain model to multiple ones, is to import tokens of other chains to the original blockchain. Such integration is usually realised by different bridging solutions, using as a core algorithm cross-chain tokens or sometimes atomic cross-chain swaps. An example is wrapped bitcoin (wBTC), which can be traded at Uniswap and at other Ethereum based DEX-s as well [2].

A further approach is to build a decentralised exchange and automated market making solution directly on the top of an L0 platform. L0 platforms are called the blockchain of blockchains, integrating several blockchains with an additional 'meta' blockchain, thus realising several interoperability solutions out-of-the-box on the platform level. Examples of L0 solutions are Cosmos or Polkadot. Building a liquidity-pool-based DEX with automated market making directly on top of an L0 platform provides the possibility that tokens from all of the integrated blockchains can be easily and efficiently traded. One prominent example is Osmosis, which is built on top of Cosmos and can integrate all tokens of all blockchains that are interoperable with Cosmos[3].

2.3 APPLICATION-SPECIFIC BLOCKCHAINS

Blockchain technology has evolved considerably since the launch of Bitcoin. In the early days, blockchains had a single-layer, or 'monolithic' design, with all their functions bundled together. However, they faced a balancing act known as the 'blockchain trilemma', the struggle to optimise decentralisation, security, and scalability simultaneously.

Decentralisation refers to the distribution of network control across multiple nodes, security focuses on the resistance to hacking, and scalability means the ability of the network to grow while maintaining transaction speed. Increasing scalability often compromises either decentralisation or security, thus the trilemma.

The concept of application-specific multi-chains has emerged to address these challenges. Unlike the original monolithic (Layer 1 or L1) blockchains, these modular blockchains delegate tasks across various specialised chains or 'modules', increasing the system's throughput without sacrificing security or decentralisation. This set-up also eases the launch of new chains, enhancing scalability. Application-specific blockchains (appchains) focus on running a single application. Unlike typical apps on traditional blockchains, appchains offer better performance and lower transaction costs. They also allow developers more customisation options, thus offering a more tailored user experience. But they do come with their own set of challenges such as increased complexity, potential resource wastage, and risk of becoming permissioned systems.

Various platforms are building multi-chain environments to further enhance interoperability, including Cosmos Zones, Polkadot Parachains, Avalanche Subnets, and Polygon Supernets. Each of these ecosystems has its unique features, security mechanisms, and native cryptocurrencies. They serve as nodes of a broader interconnected blockchain universe and are integral to paving the way for a more scalable, secure, and decentralised future.

User appchains are not to be confused with Layer 2 (L2) solutions, in which an additional blockchain is added on top of an underlying L1 to help it scale and perform some of its tasks, since appchains are focused on specific applications. In that sense, they are also different to sidechains, which have their own security protocols and post transactions on the main blockchain. As was mentioned, application-specific blockchains mainly exist in multi-chain environments, out of which the most popular and notable are listed and presented below.

[2] https://blog.liquality.io/wbtc-wrapped-btc-or-wat-btc/

[3] https://consensys.net/blog/cryptoeconomic-research/osmosis-a-fully-customizable-cross-chain-amm-built-on-cosmos/

Cosmos Zones Cosmos was introduced as the internet of blockchains, presenting the Inter-Blockchain Communication (IBC) Protocol in 2016. IBC is a specification for data transfer between arbitrary state machines, consisting of two layers. The transport layer provides the infrastructure needed to create connections between machines, and the application layer, on top of which developers can build their appchains, called zones, decides about the data management. The Cosmos Hub is a blockchain serving as the central point of this interchain ecosystem, offering a marketplace for digital assets from zones all across the network, and most importantly, operates decentralised bridges with major blockchains like Bitcoin and Ethereum. ATOM is the hub's native cryptocurrency and after an upcoming interchain security feature update, will be used to provide security across many chains via staking. Cosmos Hub is powered by Tendermint's BFT consensus algorithm, was one of the first proposed proof-of-stake consensus mechanisms focusing mainly on Byzantine fault tolerance (BFT). It should be noted that not all zones have to be linked with the hub, and some of the 277 built with the Cosmos SDK, in existence at the time of writing, do not connect to it.

Polkadot Parachains

Polkadot supports a growing ecosystem of advanced, specialised EVM compatible L1 blockchains, called parachains. All parachains are linked with a central Layer 0 blockchain (meaning that it operates on top of a bare foundational network protocol) called the relay chain. The relay chain operates using a proof-of-stake consensus protocol and being Layer 0, it does not support the composition of smart contracts, although this is possible for parachains. There are up to 100 available slots for parachains and for one to connect to Polkadot, developers need to lease a slot – after an on-chain auction lasting 1 week – on the relay chain for up to 96 weeks at a time, with the option to renew. Winners of the auction lock up a bond in DOT (Polkadot's native cryptocurrency) for the duration of the lease, and after it is over, the bond is unlocked, meaning that the unavailability of these funds represents a lost opportunity cost for alternative activities. Polkadot is also running an additional solution to increase its capacity with chains called parathreads. Parathreads are pay-as-you-go parachains, with a financial cost for each new block created, and Polkadot supports up to 10,000 parathreads. Parachains and parathreads are developed using Substrate, an SDK using Rust-based libraries and tools.

Avalanche Subnets

Subnets can be either L1 or L2 blockchains consisting of sets of nodes acting as validators assigned to one or more blockchains within the broader Avalanche network. The platform includes custom subnets and a special primary network running three separate blockchains. The first one, the C-Chain, is an instance of the Coreth virtual machine, implementing EVM, and is used for the execution of Ethereum-compatible Solidity smart contracts. The second one, the P-Chain, is an instance of the Platform virtual machine and contains validators and subnets, supporting all operations on their level, like creation of new subnets, validator allocation etc. The third one, called X-Chain, is responsible for operations on digital smart assets (meaning that they represent a real-world resource with a behaviour defined by a set of rules) known as Avalanche Native Tokens. All three chains are currently using the Avalanche consensus protocol, which is based on the Snowball algorithm, and essentially guarantees with high probability that if an initial, honest validator accepts a transaction, the rest of the honest validators will quickly come to agree with him after clustering around conflicting transactions, and will eventually accept the transaction, or if it is conflicting, reject it. All validators are required to become members of the primary network by staking 2000 AVAX, Avalanche's native cryptocurrency. The command centre for the ecosystem is called Core and provides communication with Bitcoin, Ethereum, and all EVM-compatible blockchains as well.

Polygon Supernets Polygon Labs have launched multiple scaling projects for Ethereum, like the Polygon PoS, an L2/sidechain solution, and its supernets also use Ethereum as the L1 foundation. Supernets are appchains built using Polygon Edge, a modular and extensible framework for building Ethereum-compatible blockchain networks. Supernets extend Polygon's PoS Mainnet blockspace and currently the only deployment configuration supported is that of a native bridge to the PoS rootchain. The consensus mechanism is called PolyBFT and consists of a BFT consensus engine and a proof-of-stake architecture based on the staking of MATIC, Polygon's native cryptocurrency. Supernets also have their own native gas tokens, allowing developers to provide custom fees to end users, or even relieve them from further expenses. It should be noted that each set of validator nodes only serves one supernet.

CHAPTER 3 BRIDGES- CONNECTING BLOCKCHAINS

3.1 INTRODUCTION TO BLOCKCHAIN BRIDGES

What are bridges?

Each blockchain can exist as a separate and independent network with its own token, features, and governance model which are incompatible with other blockchains. This limits the purpose of blockchains – decentralisation and scaling – leading to the creation of silos rather than an inclusive and decentralised network with their own respective advantages as well as disadvantages. Hence, it is essential to build connections between different blockchains for interaction, faster transfer of assets, decentralisation as well as technological advancements. These connections are known as bridges.

Blockchain bridges are protocols that act as pathways to allow the transfer of tokens as well as data between two or more blockchains. By providing such services bridges function as a major proponent of blockchain interoperability.

Why do we need bridges?

No blockchain is perfect, and, as the technology evolves, aggregation and interaction will be at the centre of it. All blockchains have their limitations – some have issues with scalability whereas others compromise on decentralisation for scalability, throughput, and transaction cost. Being built in isolated silos, most blockchains are unable to communicate with each other due to compatibility issues thereby limiting the potential of data or asset movement between blockchains.

Bridges enable connections between blockchains, allowing not only the transfer of information and tokens between them but also enabling access to decentralised applications on other blockchains as well as collaboration between developers of different blockchain ecosystems to build a cohesive, secure and scalable ecosystem. For example, the Arbitrum bridge has enabled bridging of assets from the Ethereum blockchain, which is plagued by high transaction costs and low scalability, to the Arbitrum blockchain, which has lower transaction costs and higher scalability as its main features.

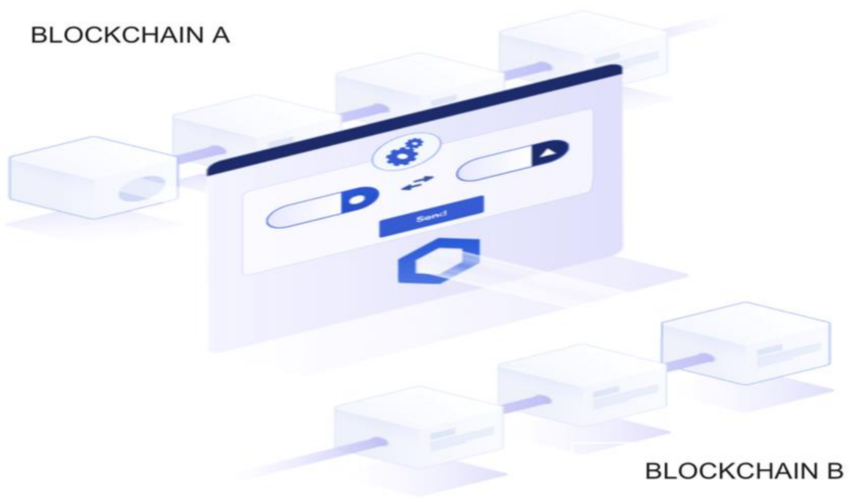

*Figure 3: Basic blockchain bridge schema. Source: https://chain.link/***Benefits of bridges**

Some of the benefits of blockchain bridges are the reason why blockchain bridges are used. Some of them are listed below.

1. Enable **exchange of assets and data** across different blockchains.
2. Enhance **scalability** by accommodating large numbers of transactions. The Arbitrum and Polygon bridges are two such examples, which are readily being used as scaling solutions for the Ethereum network.

   Bridges can be classified in a number of ways depending upon their mode of operation, functionalities, and usage. The most commonly used classifications for bridges, based on how they work, are trusted (centralised) and trustless (decentralised) bridges.

3.2 TYPES OF BRIDGES

3.2.1 TRUSTED BRIDGES

A bridge is 'trusted' if it depends on a central system for conducting its operations of asset and data transfer. The central system is manually controlled and governed, at the same time being responsible for the security of the bridge and custody of the funds. To perform operations or to execute a transaction via a trusted bridge, users have to give up control of their assets and place trust in the central system. Such bridges are suited for users prioritising lower gas fees and higher speed over cross-chain security.

Risks associated with using trusted bridges

The centralised control in trusted bridges makes it susceptible to **cybersecurity attacks** as well as illicit actions by the controlling group, as they can not only censor users from executing a transaction (**censorship risk**) but also collude to steal the user funds (**custodial risk**). Vulnerabilities in the code or error while performing a transaction or movement of data are other important risk factors.

Hence, it is imperative for users to do research prior to using any bridge to gauge the efficiency and security of the bridge.

3.2.2 TRUSTLESS BRIDGES

A bridge is a 'trustless' if it relies on smart contracts and algorithms embedded in the design of the bridge rather than a central system. With the absence of a central system to direct the bridge operations, users have full control of their assets as well as actions while executing transactions.

Trustless bridges are decentralised and secure compared to trusted bridges, though the transaction costs may be comparatively higher. They form the backbone of cross chain decentralised finance (DeFi) networks. Hop protocol. Stargate, and Wormhole Bridge are some examples of trustless bridges.

Risks associated with using trustless bridges

Trustless bridges have been around for a few years, but it is still quite early to consider them reliable to be used due to **code vulnerabilities** in the **smart contract or algorithms** that have led to multi-million dollar hacks. Any **manual error** by the user can lead to loss of funds which can be seen as a point of contention, since a trustless bridge mechanism entrusts the users with their funds. Some of the other risks associated with trustless bridges are cybersecurity risks, malicious malware risks, etc.

Bridge hacks in numbers

DeFi has seen an increase in the number of users as well as transaction volume in the last few years, with bridges playing a major role in making this possible. This has led to blockchain bridges being at the centre of attention of hackers as well. Over USD 2.5 billion have been stolen by hackers who have exploited vulnerabilities in bridges with Ronin Bridge – USD 600 million, Wormhole Hack – USD 300 million, Nomad Hack – USD 190 million, Binance hack – USD 100 million being some of the noteworthy exploitations.

3.2.3 Trusted Relay Solutions

According to Wang, Wang, and Chen (2023), a trusted relay can be conceptualised as a bridge that facilitates smart contract services across different blockchains. According to Belchior et al. (2022), the proposed scheme utilises verifiable smart contracts to replicate block information from the source blockchain onto a target blockchain. This is achieved through a blockchain registry that verifies the presence of data on the source blockchain without necessitating trust in a centralised entity. Relays facilitate the functionality of one blockchain to operate as a 'client' of another blockchain (Wang, Wang, & Chen, 2023).

Trusted relays involve reliable entities that redirect transactions from one blockchain to another (Wang, Wang and Chen, 2023). In contrast to notary schemes, trusted relays function on a chain-to-chain level without imposing trust on distributed nodes. Trusted relay schemes are commonly observed in a permissioned blockchain setting, wherein reliable escrow parties facilitate cross-blockchain transactions (Belchior et al., 2022).

A trusted relay is a simple yet effective method for promoting interoperability, allowing for easy adoption. These schemes have been found to possess high levels of usability and reliability (Wang, Wang, & Chen, 2023). They offer features such as asset portability and atomic swaps, making them applicable for complex use cases without any discernible restrictions (Wang, Wang, & Chen, 2023). However, the verification procedures in heterogeneous blockchains can exhibit significant variations, potentially leading to higher operational expenses (Wang, Wang, & Chen, 2023).

3.2.4 OTHER TYPES OF BRIDGES

In addition to classifying bridges on how they work, bridges can also be classified on the basis of what they connect, their function, the mechanism they use, as well as how they move assets. There are other designs of bridges which are classified on their functionalities as well. Some of them have been described below.

Based on the type of chains they connect

1. **L1 to L1 bridges** connect different Layer 1 (L1) blockchains with each other. For example, Avalanche Bridge connects Avalanche and Ethereum blockchains.
2. **L1/L2 to L2 bridges** connect Layer 1 to layer 2 (L2) blockchains, as well as L2 blockchains with each other. For example, Arbitrum Bridge connects Ethereum and Arbitrum blockchains, Hop Protocol connects different L2s with each other apart from connecting them to Ethereum.

Based on how they move assets

- **Lock & mint bridges** lock assets on the source chain and mint assets on the destination chain. For example, Avalanche Bridge, Wrapped BTC, etc.
- **Burn & mint bridges** burn asset on the source chains and mint asset on the destination chain, For example, Hop Protocol
- **Atomic swaps** rely on trustless, self-executing smart contracts that swap assets on the source chains with assets on the destination chain, thereby removing any requirement for third party involvement.

Based on their function

- **Wrapped asset bridges** enable transfer of non-native assets to different blockchains. A wrapped token is minted on the destination chain representing the same value as the token on the source chains. For example, wrapped BTC (WBTC), an ERC20 token compatible with the Ethereum network.
- **Multichain bridges** enable transfer between multiple blockchains, L1 and L2.

- **Chain to chain bridges** are designed to transfer assets between two specific chains and primarily use the lock and mint mechanism to move assets
- **Specialised bridges** are focused on specific ecosystems and support movement of assets in the same ecosystem, for example Ethereum and L2s on Ethereum, resulting in faster and cheaper transactions. Across is a bridge that enables such transfers from L2 rollups to Ethereum as well as XDai Bridge.

Based on mechanism
A bridge which allows assets to be transferred from one blockchain to another in one direction only is a **unidirectional bridge**, whereas a bridge that facilitates asset transfer in both directions is known as a **bidirectional bridge**. Wrapped BTC is an example of a unidirectional bridge while Avalanche Bridge is an example of a bidirectional bridge.

Based on control of assets

1. **Custodial bridges** require users to place their trust in a central entity to operate the system and relinquish control of their assets. Binance Bridge is an example of a custodial bridge.
2. **Non-custodial bridges** rely on smart contracts to manage the crypto locking and minting processes, thereby removing the need for a central system. Non-custodial bridges are decentralised and comparatively more secure. Hop Protocol is an example of a non-custodial bridge.

3.3 OVERVIEW OF THE LEADING BLOCKCHAIN BRIDGES

As per latest data on DeFi Lama, USD 10.7 billion worth of crypto assets are locked on bridges and USD $4.27 billion worth of wrapped BTC (WBTC). The TVL on bridges was at its peak in Q2 2022, above USD 30 billion, but due to multiple hacks and issues that occurred in the latter half of the year in the crypto space, a steep decline in the TVL on bridges was unavoidable. As of today, the market for cross-chain bridges is highly competitive and in continuous evolution. The landscape encompasses bridges like Stargate, Arbitrum Bridge, Polygon PoS Bridge, Celer cBridge, Avalanche Bridge, Multichain, Synapse, Hop, xDai Bridge, Optimism Gateway, Portal by Wormhole, Core Bitcoin Bridge, Rainbow Bridge, and Across.

Although the overall market is quite fragmented, a comprehensive analysis on DefiLlama revealed that four main players dominate the market. Indeed, Polygon PoS Bridge, Stargate, Arbitrum Bridge, and Multichain (formerly Anyswap) cover 69% of the bridge market. Their total volume of transactions since 1 September 2022 are: USD 16.45 billion (Polygon), USD 8.44 billion (Stargate), USD 7.08 billion (Arbitrum), and USD 9.41 billion (Multichain), adding up to a total of USD 41.38 billion.

In the past few months, we have seen movement of a lot of liquidity from Ethereum to numerous blockchains such as Optimism, Arbitrum, Fantom, Avalanche, Polygon, etc. This migration of funds has been aided by bridges, thus providing users with access to multiple DeFi platforms and enabling them to execute their transactions faster and at lower cost. The most prominent bridges are Stargate, Arbitrum Bridge, Avalanche Bridge, Wormhole Bridge, Celer Bridge, etc. Each of these bridges provides avenues for interoperability among major blockchain protocols for the exchange of assets, as well for technical advancement collaboration.

Name	Chains	1d Change	24h Volume	7d Volume	1m Volume	24h # of Txs
1 Stargate		-2.49%	$60.46m	$826.47m	$2.65b	269602
2 Arbitrum Bridge		+53.41%	$11.75m	$223.7m	$987.4m	956
3 Core Bitcoin Bridge		+428%	$4,360,905	$27.23m	$59.19m	72
4 Hop		-36.29%	$2,750,505	$26.89m	$108.29m	2766
5 Across		-29.90%	$1,642,149	$23.53m	$99.72m	1023
6 Celer cBridge		-66.10%	$1,246,238	$72.99m	$267.15m	1745
7 Polygon PoS Bridge		-63.80%	$1,245,889	$198.1m	$4.13b	526
8 Synapse		-32.24%	$1,210,797	$24.37m	$130.76m	451
9 Optimism Gateway		-44.15%	$714,482	$48.6m	$200.08m	262
10 Avalanche Bridge		+250%	$588,187	$20.38m	$69.45m	60
11 Portal by Wormhole		+60.00%	$288,846	$16.84m	$125.73m	472

Figure 4: List of blockchain bridges. Source: https://defillama.com/bridges

NOTABLE BRIDGES

WBTC Bridge enables transfer of bitcoin to the Ethereum network to enhance the liquidity of Ethereum and provide an avenue to standardise bitcoin to the ERC20 format, which makes it easier to integrate bitcoin into smart contracts. This bridge can be classified as a mint and burn bridge with trusted custodians to govern transaction execution. The WBTC Bridge has the highest TVL -approximately USD 4 billion, which represents half of the total deposits of bridged assets.

Stargate Bridge is a trustless bridge with a vision to make cross-chain liquidity transfer a seamless, single transaction process. It was the first bridge to tackle the bridging trilemma of instant guaranteed finality, use of native assets (not wrapped), and unified liquidity across multiple chains. Prominent blockchains for which transfers have been enabled via Stargate Bridge are Ethereum, Binance. Avalanche, Polygon, Arbitrum, Optimism, and Fantom. The TVL for Stargate Bridge is USD 409 million

Wormhole Bridge is a one-stop platform to bridge assets and messages between different blockchain protocols, with Ethereum, Binance, Solana, and Polygon being the prominent blockchains, among others. The Wormhole bridge is more than a generic interoperability protocol, it is also an ecosystem and platform for developers to grow the decentralised computing space. Wormhole consists of multiple modular swap-in components that can be leveraged independently and supports an increasing number of composable applications built by numerous teams. The Wormhole project started as a trusted bridge between Ethereum and Solana in 2020, but since then has evolved into a trustless bridge that can be used to transfer assets and messages across multiple chains. The TVL for the Wormhole bridge is USD 358, while the message volume parsed is 405 million.

Avalanche Bridge provides a quick, secure, and low-cost way to bridge assets between Avalanche and Ethereum. It is a trusted bridge with a TVL of USD 198 million.

3.4 LIMITATIONS ON BUILDING BRIDGES

Building secure and efficient bridges between blockchains for the interoperability needed to move assets as well as data across chains is very difficult. It would be a good idea to build specialised bridges to minimise risks and get maximum efficiency. There are multiple factors to be weighed while building blockchain bridges – security, transaction costs, decentralisation, speed of transaction, cybersecurity, smart contract audit, platform audit, user know-how of platform usage, etc. Trade-offs are considered when building solutions suitable for the requisite applications, but we are far from getting the best possible solution.

Precautionary measures to be considered

Bridges are an integral part of DeFi and, by extension, the Web3 ecosystem, irrespective of the architecture or consensus of the blockchains, since it facilitates the transfer of a substantial amount of DeFi trading volumes. Hence, it is important to not only work on advancing the bridge designs but simultaneously on building a robust risk management system to safeguard against software vulnerabilities as well as hacking.

Thus, important preventive measures that developers should consider before launching public usage are smart contract audits to check for code vulnerabilities and thorough platform audits to test the security of the platform and attached interfaces against known issues that have already occurred in the past.

CHAPTER 4 THE FUTURE OF BLOCKCHAIN INTEROPERABILITY

4.1 OPPORTUNITIES THROUGH BLOCKCHAIN INTEROPERABILITY

1) Technology Convergence

The convergence of technologies is a growing trend, transforming how we interact with the world.

The engineering field is continuously evolving with new technologies and innovations. A few emerging megatrends in engineering are set to shape the future of science and technology, with forecasted broad impact on society and the economy, such as 6G or 10G networks, satellite internet, digital twins, and quantum computing, among others.

‘Blockchain technologies now offer broad opportunities to improve efficiency, security, and transparency for sensitive data systems. Applications in artificial intelligence are emerging, for example federated learning over secure decentralised storage are enabling multi-party collaborations for model development are now viable. As advances in neuromorphic and quantum disrupt traditional computing paradigms, we anticipate that new blockchain technologies will be critical to the management and security of these new architectures, benefit from post-quantum encryption and key management schemes and contribute to the security fabric for internet scale applications’ said Dr Yelena Yesha, Knight Foundation Endowed Chair of Data Science and AI.

A paper published on the value of 6G networks for blockchain (Shen et al., *Engineering*, 2022) addresses the challenges and opportunities in blockchain deployments in 6G-powered data exchanges, which will be vital for a maturing interoperable blockchain ecosystem. The authors explore the consensus protocols and scalability mechanisms in blockchains and discuss the roles of various stakeholders in blockchain architectures. They also investigate the authentication and authorisation requirements and critical privacy requirements.

Blockchain interoperability could act as an enabler for digital twin technologies or quantum computing deployments. Digital twin technologies, which involve creating a virtual replica of a physical asset or system, are being used to improve the efficiency and productivity of industrial processes. Quantum computing, on the other hand, promises to revolutionise computing by providing a platform for solving complex problems beyond traditional computers' capabilities. In addition, blockchain technology provides a secure and decentralised platform for storing and managing data, while also triggering the development of novel business models and additional revenue channels.

Optimal blockchain interoperability will be critical for the successful convergence of these technologies. Blockchain interoperability could enable different networks to communicate and share information, creating a seamless ecosystem that facilitates data exchange and value. For example, digital twin technologies could leverage blockchain technology to enable secure and decentralised access to data, facilitating the creation of more efficient and resilient industrial processes. Quantum computing could also benefit from blockchain interoperability, enabling the creation of secure and decentralised networks to solve complex problems.

2) Transition to Web 3.0:

The next generation of the internet has been labelled Web 3.0 and will be defined by several converging technologies, including blockchain. However, interoperability within this novel technology architecture will be critical for the success of Web 3.0, as well as Web 4.0 and beyond, enabling different networks to communicate and share information.

By creating a seamless ecosystem of decentralised applications and services in the next iterations of the world wide web, different blockchain networks will be able to communicate and share information, therefore creating more efficient and effective decentralised applications.

3) Development of Smart Global Ecosystems

Smart global ecosystems represent the next generation of interconnected systems, enabling the seamless exchange of data and value across different industries and regions. Blockchain technology is a crucial enabler of these new ecosystems, providing a secure and decentralised platform for the exchange of data and value. However, interoperability is critical for their success, enabling different networks to communicate and share information.

Blockchain interoperability enables the creation of smart global ecosystems, enabling different networks to communicate and share information, creating a seamless ecosystem that facilitates the exchange of data and value (Mathur et al, *Computer Networks*, 2023). Blockchain interoperability could create a global supply chain management system, enabling the seamless exchange of information and value across different regions and industries. Blockchain interoperability also enables the creation of a global identity management system, enabling the seamless exchange of identity information across different industries and regions.

4) Creator Economy

The evolving blockchain technology is transforming the creator economy by enhancing transparency, accountability, and trust. Maturing blockchain interoperability will enhance cross-chain transactions' capacity, scalability, and security, enabling the seamless exchange of value and data across different blockchain platforms in this newly configured economy. One central value would be the ability to monetise content across different blockchain networks, creating new revenue streams and reducing transaction costs. We can also expect an improvement in the transparency and accountability of creators' income, ensuring that creators receive fair compensation for their work. A more mature interoperable blockchain ecosystem could also develop new applications and use cases for blockchain technology in this novel economy, enhancing the efficiency and effectiveness of creator-related transactions.

A paper published on the democratising effects of distributed ledger technologies (Makridis et al., *Frontiers*, Vol.6, 2023), emphasises their democratising effects and highlights the implications for economic mobility. The authors offer a few pathways for how distributed ledger technologies can influence labour, competition, and economic outcomes, such as the creation of new and higher value-added jobs, the modularisation of complex tasks, improvements in the way people learn and acquire human capital, increased competition in the marketplace, and more inclusive access to financial services with fewer intermediaries.

5) Accelerating a Net Zero Economy:

The transition to a net-zero economy is a global imperative, requiring the creation of new business models and technologies that enable the decarbonisation of different industries. Blockchain technology can be a powerful catalyst of the net-zero economy, providing a secure and decentralised platform for exchanging data and unlocking the ROI. However, interoperability is critical for the success of the net-zero economy, enabling different networks to communicate and share information and value.

For example, enhanced blockchain interoperability could lead to a decentralised energy marketplace, enabling the seamless exchange of renewable energy credits and creating more efficient and sustainable energy systems. Blockchain interoperability could also be foundational to creating a carbon offset marketplace, enabling the seamless exchange of carbon credits, and facilitating the transition to a carbon-neutral economy.

‘Blockchain tech and smart contracts may help give impetus to grid modernisation and reduce the need for many third parties to facilitate the adoption and monetisation of distributed energy transactions and exchanges, both data and energy flows as well as financial transactions’, said Dr Michael Mylrea, distinguished fellow at the University of Miami’s Institute of Data Science & Computing. ‘This may help reduce transactive energy costs and increase the security and sustainability of distributed energy resource (DER) interoperability enabling a more decentralised and resilient power grid’.

To be sustainable, blockchain interoperability will demand the creation of new business models and new financing instruments. Additionally, new international interoperability standards, custom KPIs, and metrics will need to be designed and monitored.

6) Metaverse and Omniverse Economy

Blockchain interoperability can also create new ecosystems, such as the metaverse(s) and the industrial metaverse or the omniverse (Mourtsis et al, *Applied Sciences*, 2023), which will transform how we interact with the world, creating a more efficient, sustainable, and equitable future (Truong et al, *IEEE Access*, 2023). As with other frontier technologies, we can expect blockchain solutions to continuously evolve, mature, and adapt to the global ecosystem. Interoperability will remain a key priority, enabling new opportunities and unlocking the full potential of blockchain technology.

A recent comprehensive review of blockchain deployments for the metaverse (Thien Huynh-The et al., *Science Direct*, 2023) emphasises that data security is paramount. The authors highlight that blockchain technology presents a promising solution due to its unique decentralization, immutability, and transparency features. They also describe the impact of data acquisition, storage, sharing, interoperability, and privacy preservation. They identify the technical challenges for each perspective and illustrate how blockchain can address them. Additionally, they explore the impact of blockchain on critical enabling technologies for the metaverse, such as the Internet-of-Things, digital twins, multi-sensory and immersive applications, artificial intelligence, and big data. The authors also showcase significant projects demonstrating blockchain's role in metaverse applications and services. Finally, we suggest promising research directions to further advance the use of blockchain technology in the metaverse in the future.

Directions for Future Research

Further research could be dedicated to the potential to revolutionise global data exchanges and data centres by enabling secure, decentralised, and efficient data sharing across different networks and industries. Optimal blockchain interoperability could be foundational for global data exchanges, enhancing the efficiency and transparency of data transfers and reducing the risks associated with centralisation and data breaches.

Interoperability between blockchain networks also enables the seamless exchange of data across different industries, enabling the creation of global exchanges that facilitate the exchange of data and value across different regions and sectors. For example, blockchain interoperability could facilitate the creation of a global health data exchange, enabling the secure and decentralised sharing of patient data and medical records across different healthcare providers and regions. Similarly, blockchain interoperability could facilitate the creation of a global financial data exchange, enabling seamless transactions across different financial institutions and regions.

In addition to enhancing global data exchanges, blockchain interoperability can also improve the efficiency and security of global data centres. By enabling secure and decentralised access to data across different networks, blockchain interoperability can reduce the risks associated with centralised data storage and improve the resilience of data centres to cyber threats and data breaches. Interoperability can also enhance the transparency and accountability of data management, enabling more efficient and effective monitoring and auditing of data centres.

4.2 CONCLUSIONS

In conclusion, blockchain interoperability holds tremendous potential for unlocking return on investment and amplifying the impact of global science and tech-diplomacy efforts toward creating a more prosperous and equitable world. Interoperability can enhance the trust and efficiency of multi-party collaborations, increase the value of data sharing, and drive innovation in various applications. Through interoperability, we can harness the power of blockchain networks to solve complex global challenges such as climate change, financial inclusion, and healthcare access.

Furthermore, the development of blockchain interoperability can create new business models and opportunities, particularly in the creator economy. The ability to quickly transfer value and content across different blockchain networks will drive innovation and growth in creative industries such as music, art, and gaming. Blockchain-based solutions enable creators to monetise their content in new ways and empower them to have greater control over their intellectual property.

However, the journey towards blockchain interoperability is challenging. The complexity of underlying architectures, varying consensus mechanisms, and governance structures pose significant obstacles. Overcoming these challenges will require concerted efforts from researchers, developers, policymakers, and industry players to establish common standards and protocols.

To fully unlock the potential of blockchain interoperability, we must also ensure that it is developed responsibly and ethically. This involves addressing data privacy, security, and governance issues and ensuring that interoperability's benefits are distributed equitably across different stakeholders.

REFERENCES

5 Biggest Crypto Cross-Chain Bridge Hacks in 2022. (n.d.). https://bitcoin.tax/blog/cross-chain-bridge-hacks/.

Abebe, E., Behl, D., Govindarajan, C., Hu, Y., Karunamoorthy, D., Novotny, P., Pandit, V., Ramakrishna, V. and Vecchiola, C. (2019). Enabling Enterprise Blockchain Interoperability with Trusted Data Transfer (Industry Track). *Proceedings of the 20th International Middleware Conference Industrial Track.* https://doi.org/10.1145/3366626.3368129

Anuska. (2023). 8 Best Cross-Chain Bridges for 2023. *Shardeum Blogs* | *EVM-based Sharded L1 Blockchain*. https://shardeum.org/blog/best-cross-chain-bridges/#List_of_Cross-Chain_Bridges

Avalanche bridge — bridge between 2 networks, $1 199 005 328 total TVL - 1 reviews — Chainspot. (n.d.). https://chainspot.io/bridge/avalanche-bridge

Avalanche Dev Docs: Create Without Limits. (n.d.-a). https://docs.avax.network/learn/avalanche/avalanche-platform

Avalanche Dev Docs: Create Without Limits. (n.d.-b). https://docs.avax.network/learn/avalanche/avalanche-consensus

Barbàra, F. and Schifanella, C. (2023). 'MP-HTLC: Enabling blockchain interoperability through a multiparty implementation of the hash time-lock contract,' *Concurrency and Computation: Practice and Experience*, 35(9). https://doi.org/10.1002/cpe.7656

Belchior, R., Vasconcelos, A., Guerreiro, S. and Correia, M. (2022). A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Computing Surveys*, 54(8), pp.1–41. https://doi.org/10.1145/3471140

Berenzon, D. (2022, October 5). Application-Specific Blockchains: The Past, Present, and Future. *Medium*. https://medium.com/1kxnetwork/application-specific-blockchains-9a36511c832

Besancon, L., Da Silva, C. F., Ghodous, P., & Gelas, J. (2022). A Blockchain Ontology for DApps Development. *IEEE Access*, *10*, 49905–49933. https://doi.org/10.1109/access.2022.3173313

Besançon, L., Ferreira, C. and Parisa Ghodous (2019). Towards Blockchain Interoperability: Improving Video Games Data Exchange. *HAL (Le Centre pour la Communication Scientifique Directe).* https://doi.org/10.1109/bloc.2019.8751347

Bishnol, M. and Bhatia, R. (2020). Interoperability Solutions for Blockchain. *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE).* https://doi.org/10.1109/icstcee49637.2020.9277054

Build your own blockchain, without the complexity. (n.d.). https://polygon.technology/polygon-supernets

Buterin, V. (2016). Chain Interoperability. Available at: https://allquantor.at/blockchainbib/pdf/vitalik2016chain.pdf

Chand, A. (2023, January 2). What Are Blockchain Bridges And How Can We Classify Them? *Medium*. https://blog.li.fi/what-are-blockchain-bridges-and-how-can-we-classify-them-560dc6ec05fa?gi=87c114023779

CoinMarketCap. (2022). Modular vs Monolithic Blockchains: What's the Difference? *CoinMarketCap Alexandria*. https://coinmarketcap.com/alexandria/article/modular-vs-monolithic-blockchains-what-s-the-difference

Cosmos. (2019, January 30). *cosmos/WHITEPAPER.md at master · cosmos/cosmos*. GitHub. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md#tendermint-bft

Cosmos: The Internet of Blockchains. (n.d.). Cosmos: The Internet of Blockchains. https://cosmos.network/

Cross-Chain Interoperability Protocol (CCIP) | *Chainlink*. (n.d.). https://chain.link/cross-chain

Dai, B., Jiang, S., Zhu, M., Lu, M., Li, D. and Li, C. (2020). Research and Implementation of Cross-Chain Transaction Model Based on Improved Hash-Locking. *Communications in Computer and Information Science*, pp.218–230. https://doi.org/10.1007/978-981-15-9213-3_17

DefiLlama. (n.d.-a). DefiLlama. https://defillama.com/protocols/Bridge

DefiLlama. (n.d.-b). DefiLlama. https://defillama.com/bridges

DefiLlama. (n.d.-d). DefiLlama. https://defillama.com/bridge/multichain

DefiLlama. (n.d.-e). DefiLlama. https://defillama.com/bridge/stargate

Ellis, S., Juels, A., & Nazarov, S. (2017). *ChainLink A Decentralized Oracle Network*. https://research.chain.link/whitepaper-v1.pdf

Ethereum. (n.d.-a). *Introduction to blockchain bridges | ethereum.org*. ethereum.org. https://ethereum.org/en/bridges/

Ethereum. (n.d.-b). *Introduction to the Ethereum stack | ethereum.org*. ethereum.org. https://ethereum.org/en/developers/docs/ethereum-stack/

Fáwọlé, J. (2023). Blockchain Bridges 101: How Do They Work? *Hacken*. https://hacken.io/discover/blockchain-bridges/

Fynn, E., Bessani, A. and Pedone, F. (2020). Smart Contracts on the Move. *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).* https://doi.org/10.1109/dsn48063.2020.00040.

Gadekallu, T. R. (2022, March 18). *Blockchain for the Metaverse: A Review*. arXiv.org. https://arxiv.org/abs/2203.09738

Hang, L., Jamil, F., Jin, W., Kahng, H.-K., Kim, S. and Kim, D.-H. (2020). Transaction Data Control for Blockchain Networks. In: *The 4th International Conference on Interdisciplinary Research on Computer Science, Psychology, and Education (ICICPE 2020)*. https://www.researchgate.net/publication/348210683_Transaction_Data_Control_for_Blockchain_Networks

Herlihy, M. (2018). Atomic Cross-Chain Swaps. *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*. https://doi.org/10.1145/3212734.3212736

Hueber, O. (2018). The blockchain and the sidechain innovations for the electronic commerce beyond the Bitcoin's framework. *International Journal of Transitions and Innovation Systems*, *6*(1), 88. https://doi.org/10.1504/ijtis.2018.090770

Hyperledger Foundation. (2022, November 7). *Hyperledger Cacti – Hyperledger Foundation*. https://www.hyperledger.org/use/cacti

Inter-Blockchain Communication. (n.d.). https://ibcprotocol.dev/

Interledger.org. (2023). *Interledger Protocol (ILP): Overview.* [online] Available at: https://interledger.org/developer-tools/get-started/overview/

Introduction - Wormhole Development Book. (n.d.). https://book.wormhole.com/

Khan, S., Amin, M.B., Azar, A.T. and Aslam, S. (2021). Towards Interoperable Blockchains: A Survey on the Role of Smart Contracts in Blockchain Interoperability. *IEEE Access.* https://doi.org/10.1109/access.2021.3106384

Kotey, S. D., Tchao, E. T., Ahmed, A., Agbemenu, A. S., Nunoo-Mensah, H., Sikora, A., Welte, D., & Keelson, E. (2023). Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. *Iet Communications*. https://doi.org/10.1049/cmu2.12594

Liquality. (2022). WBTC: Wrapped BTC or Wat BTC? *Liquality Blog: Unlock the Value of Web3*. https://blog.liquality.io/wbtc-wrapped-btc-or-wat-btc/

Liu, F., He, S., Li, Z., Xiang, P., Qi, J. and Li, Z. (2023). An Overview of Blockchain Efficient Interaction Technologies. *Frontiers in Blockchain*, 6. https://doi.org/10.3389/fbloc.2023.996070

Makridis, C. (2022). Democratizing Effects of Digital Ledger Technologies: Implications for Economic Mobility. *SSRN*. https://doi.org/10.2139/ssrn.4134834

Mathur, S., Kalla, A., Gür, G., Bohra, M. K., & Liyanage, M. (2023). A Survey on Role of Blockchain for IoT: Applications and Technical Aspects. *Computer Networks*, *227*, 109726. https://doi.org/10.1016/j.comnet.2023.109726

Miller, F., Kuzmyn, N., & Lawler, C. (2023). Best Cross-Chain Bridges for Moving Cryptocurrency Across Different Blockchains. *DailyCoin*. https://dailycoin.com/best-cross-chain-bridges-in-crypto/#:~:text=Synapse,choice%20for%20first-time%20bridges

Min, A. (2020). Atomic Swaps Explained: Swap Cryptocurrencies P2P Without Mediation. *Liquality Blog: Unlock the Value of Web3*. https://blog.liquality.io/atomic-swaps-explained/

Modular vs. Monolithic Blockchains. (n.d.). https://www.alchemy.com/overviews/modular-vs-monolithic-blockchains

Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). Blockchain Integration in the Era of Industrial Metaverse. *Applied Sciences*, *13*(3), 1353. https://doi.org/10.3390/app13031353

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System (white paper). https://bitcoin.org/bitcoin.pdf

Parachains | *Next-Generation Blockchains* | *Polkadot*. (n.d.). Polkadot Network. https://polkadot.network/features/parachains/

*Permissioned Distributed Ledger (PDL) ; Inter-Ledger interoperability (*DGR/PDL-006_Interop)

GR PDL 006 - V1.1.1 - Permissioned Distributed Ledger (PDL); Inter-Ledger interoperability (etsi.org)

Polkadot Parachain Slot Auctions | *Polkadot*. (n.d.). Polkadot Network. https://polkadot.network/features/auctions/

Qasse, I.A., Abu Talib, M. and Nasir, Q. (2019). Inter Blockchain Communication. *Proceedings of the ArabWIC 6th Annual International Conference Research Track on - ArabWIC 2019.* https://doi.org/10.1145/3333165.3333167

Santini, P. (2022, January 20). *Optimization of a Reed-Solomon code-based protocol against blockchain data availability attacks*. arXiv.org. https://arxiv.org/abs/2201.08261

Schulte, S., Sigwart, M., Frauenthaler, P. and Borkowski, M. (2019). Towards Blockchain Interoperability. *Business Process Management: Blockchain and Central and Eastern Europe Forum*, pp.3–10. https://doi.org/10.1007/978-3-030-30429-4_1

Shen, X., Liu, D., Huang, C. Z., Xue, L., Yin, H. D., Zhuang, W., Sun, R., & Ying, B. (2022). Blockchain for Transparent Data Management Toward 6G. *Engineering*, *8*, 74–85. https://doi.org/10.1016/j.eng.2021.10.002

Shuttleworth, D. (2022a, March 21). *Osmosis: A Fully Customizable, Cross-Chain AMM Built on Cosmos* | *ConsenSys*. ConsenSys. https://consensys.net/blog/cryptoeconomic-research/osmosis-a-fully-customizable-cross-chain-amm-built-on-cosmos/

Shuttleworth, D. (2022b, March 28). *Stargate: a Fully Composable Cross-Chain Bridge* | *ConsenSys*. ConsenSys. https://consensys.net/blog/cryptoeconomic-research/stargate-a-fully-composable-cross-chain-bridge/

Siris, V.A., Nikander, P., Voulgaris, S., Fotiou, N., Lagutin, D. and Polyzos, G.C. (2019). Interledger Approaches. *IEEE Access*, 7, pp.89948–89966. https://doi.org/10.1109/access.2019.2926880

Stargate. (n.d.). https://stargate.finance/

Stevens, R. (2023, May 11). What Are Blockchain Bridges and How Do They Work? *CoinDesk*. https://www.coindesk.com/learn/what-are-blockchain-bridges-and-how-do-they-work/

Trivedi, C., Rao, U. P., Parmar, K., Bhattacharya, P., Tanwar, S., & Sharma, R. (2023). A transformative shift toward blockchain-based IoT environments: Consensus, smart contracts, and future directions. *Security and Privacy*. https://doi.org/10.1002/spy2.308

Truong, V. T., Le, L. B., & Niyato, D. (2023). Blockchain Meets Metaverse and Digital Asset Management: A Comprehensive Survey. *IEEE Access*, *11*, 26258–26288. https://doi.org/10.1109/access.2023.3257029

Wang, G., Wang, Q., & Chen, S. (2023). Exploring Blockchains Interoperability: A Systematic Survey. *ACM Computing Surveys*. https://doi.org/10.1145/3582882

WBTC Wrapped Bitcoin an ERC20 token backed 1:1 with Bitcoin. (n.d.). Wrapped Bitcoin. https://wbtc.network/

What is an application-specific blockchain (appchain)? (n.d.). https://www.alchemy.com/overviews/what-is-an-appchain

What is the Blockchain Trilemma? | Ledger. (2023, May 29). Ledger. https://www.ledger.com/academy/what-is-the-blockchain-trilemma

Wormhole. (n.d.). *Wormhole*. https://wormhole.com/

Zhang, J., Gao, J., Li, Y., Chen, Z., Guan, Z. and Chen, Z. (2022). Xscope: Hunting for Cross-Chain Bridge Attacks. *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*. https://doi.org/10.1145/3551349.3559520

Zhu, S., Chi, C. and Liu, Y. (2023). A Study on the Challenges and Solutions of Blockchain Interoperability. *China Communications*, pp.1–18. https://doi.org/10.23919/jcc.2023.00.026