Review



# Blockchain Interoperability for Future Telecoms

Suha Bayraktar *, Sezer Gören, Tacha Serif

Posted Date: 29 January 2025

doi: 10.20944/preprints202501.2195.v1

Keywords: Blockchain; Hyperledger; Interoperability; Permissioned; SAGIN; Telecommunications; 6G

*Review*

# Blockchain Interoperability for Future Telecoms

**Suha Bayraktar [1,*], Sezer Gören [2] and Tacha Serif [3,*]**

[1] Computer Engineering, Yeditepe University, Istanbul, Türkiye
[2] Computer Engineering, Umass Dartmouth
[3] Computer Engineering, Yeditepe University, Istanbul, Türkiye
* Correspondence: sbayraktar@cse.yeditepe.edu.tr (S.B.); tserif@cse.yeditepe.edu.tr (T.S.)

**Abstract:** The inherent characteristics of blockchain, including immutability, self-execution, and removing intermediaries, consistently generate increasing interest in its applications within the telecom sector, making it an exciting area for investment. This literature review article aims to explore a promising research area known as blockchain interoperability. Interoperability seeks to connect two or more independent blockchains to exchange information. By leveraging the interoperability features of blockchain, independent telecom networks can seamlessly share information with other mobile, fixed, and next-generation networks. This results in improved security, efficiency, cost savings, and an enhanced customer experience. This study reviews highly cited research papers and literature to assess blockchain's relevance to telecom use cases for interoperability. Additionally, it presents prominent interoperability solutions and identifies essential requirements for successful blockchain interoperability implementation in the telecom sector. The findings highlight key research gaps and future directions for blockchain adoption in telecommunications, particularly for the forthcoming 6G.

**Keywords:** Blockchain; Hyperledger; Interoperability; Permissioned; SAGIN; Telecommunications; 6G

## 1. Introduction

With the rise of 6G networks and innovative cloud-based, open, and flexible self-executing telecom solutions like open RAN (Radio Access Network) [1–3], telecom networks will become more adaptable and capable of automatically extending their capacity for much more extensive use cases. The Internet of Everything (IoE) will be fully realized in 6G, bringing many next-generation devices to the networks. Such a flexible and complex architecture demands robust security and access features. In this context, blockchain is anticipated to play a crucial role in the future of telecom. Furthermore, blockchain can enhance secure interoperability in telecommunications by enabling various telecom networks and systems to connect and exchange data effortlessly. According to Georgios et al. [1], while 5G has enabled the Internet of Everything (IoE), 6G will tackle numerous limitations of 5G and further improve the Internet of Things (IoT). This is anticipated to result in a vast increase in the number of devices connected to mobile networks. Such growth has significant potential to introduce major security challenges in 6G. Additionally, the requirement for seamless access for these IoE devices to other networks as they move through air, sea, and space poses further challenges. Ramraj et al. [2] contend that various technologies, including quantum computing, AI, and blockchain, will be utilized to overcome these challenges, primarily focusing on ensuring the security, confidentiality, and privacy of 6G networks.

### *1.1. Problem Statement and Motivation*

Most research on blockchain use cases in future telecom technologies focuses on deploying a single blockchain and its interoperability with internal applications through dApps. According to Ren et al. [39], blockchain interoperability operates at three distinct levels:

 doi:10.20944/preprints202501.2195.v1



- A:Among blockchain and other systems
- B:Among dApps on the same blockchain
- C:Among different blockchains

In Figure 1, the three levels of blockchain interoperability are illustrated according to Ren et al.'s [39] description. Levels A and B are integral to research projects in existing and future telecom technologies. Relevant literature, such as [3], is an example of these research projects that demonstrate interest in using blockchain in Telecoms. In [3], the authors propose dynamic spectrum allocation in 6G using a Level A oracle [7,8], which they call intermediaries. Additionally, [3] covers a use case for the interoperability of Level B using dApps [15,16] in the same research project. There is limited research and almost no studies on the interoperability of independent blockchains (Level C) operating across different telecom networks. This lack of research motivates this literature review to explore the level C type of blockchain interoperability and its use cases in telecommunications. This literature review's primary aim is to emphasize this research area's critical aspects and propose future directions, particularly for Level C interoperability use cases. Using blockchain interoperability architecture, particularly for Level C use cases, telecommunications providers can tackle the challenges of fragmented data and interoperability issues with their external partners, including roaming, interconnection, and ecosystem partners. In current telecom practices, employing Trusted Third Parties (TTPs) is a common method whenever data exchange between two or more telecom operators is required.

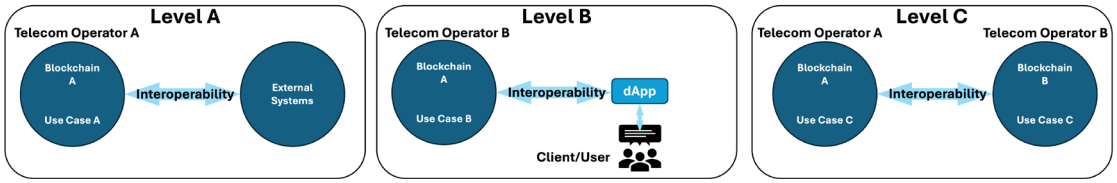



**Figure 1.** Three Levels of Blockchain Interoperability in Telecom.

On the other hand, TTPs are vulnerable to security issues, censorship, and privacy concerns. Blockchain technology can facilitate reliable peer-to-peer transactions without compromising security or privacy by removing the need for trusted intermediaries. Utilizing blockchain interoperability architecture allows telecommunications providers to unlock new opportunities for securely and efficiently connecting and exchanging information between diverse networks and systems. Another emerging area of interoperability research is becoming a vital part of decentralized organizations, especially in Web3 [9,10], and is increasingly recognized as essential for the Metaverse [11]. Assuming that both Web3 and the Metaverse will be part of future telecom networks, the significance of this literature review becomes much more critical for researchers.

### *1.2. Research Methodology of the Literature Review*

This study begins by demonstrating the history of blockchain technologies by highlighting critical technological improvements in the blockchain domain, including significant milestones new blockchain technologies have achieved. Finally, it illustrates how blockchain become an essential technology for enterprise use cases by introducing interoperability. Next, it explains why telecoms require blockchain interoperability (i.e., cross-chain communication). Critical telecom interoperability use cases that significantly influence the industry's future, including their benefits and challenges, are also illustrated. Key research papers were reviewed to provide more precise guidance for researchers in this field, highlighting essential features that can be crucial in selecting the ideal solution for telecom use cases. Next, chosen solutions are compared to assess their alignment with the highlighted features. In conclusion, a comparison table illustrates the most effective solutions based on the feature set and findings from the literature review. The research contributions are also outlined, and key topics and challenges for future discussions are highlighted.

 doi:10.20944/preprints202501.2195.v1



This literature review concludes that the research area for telecom interoperability is still in its early stages, especially concerning future 6G deployments.

### *1.3. History of Blockchain & Interoperability*

Blockchain networks were initially designed to function as standalone decentralized solutions. A decentralized approach eliminates trusted parties and provides an automatic and immutable transaction-proof system. The idea of blockchain was first offered by the inventor of Bitcoin 12, Satoshi Nakamoto 12, as a decentralized, public, permissionless, standalone, hashed-block-based cryptographic proof system that eliminates trusted parties from payment verification. There are two main types of blockchain systems: permissionless and permissioned. Permissionless blockchains operate as public networks and allow members to join without requiring approval. This design approach plays a significant role in decentralized blockchain solutions and serves as a reference blueprint for blockchain-based cryptocurrency solutions. As public permissionless blockchain designs initially focused on cryptocurrency and standalone networks, the demand for general blockchain interoperability was minimal until new popular cryptocurrencies such as Ethereum [13] were launched. Meanwhile, three well-known challenges have emerged in the research area: security, adaptation flexibility, and performance.

According to [14], the Bitcoin consensus algorithm is a widely debated topic in the Bitcoin research community due to its stability, security, and concerns regarding computational resource wastage. Ethereum was developed and launched by Buterin et al. [15] in 2015 to address some of these challenges. It aimed to provide flexibility to cryptocurrency networks by introducing Smart Contracts [15] that enable more adaptable transaction processing. The introduction of Smart Contracts has facilitated the integration of enterprise rules and application usage. Through Smart Contracts, new enterprise-based features can be added to the current consensus mechanism, such as the Proof of Work (PoW) and Proof of Stake (PoS). Finally, a new concept called Decentralized Applications (dApps) [16] enables public blockchain networks to interact flexibly with other applications. dApps were introduced within the Ethereum projects, allowing interaction with centralized and decentralized external applications using smart contracts. The introduction of Smart Contracts and dApps has also facilitated extended use cases beyond cryptocurrency deployments and has become a significant use case for various industries. Although Ethereum is a more flexible solution, Yakovenko proposed Solana [17] in 2016 to provide more high-performance blockchain-based cryptocurrency networks to address well-known performance challenges. With the effect of the newly launched cryptocurrency networks, interoperability projects have emerged for public cryptocurrency-based blockchains. Such projects were primarily built to meet the growing demand for transferring or swapping cryptocurrency assets between networks. According to [18], over 10,000 blockchain networks were reached by 2022, and significant amounts are still being built for public cryptocurrency projects.

New cryptocurrency-based interoperability projects, such as Cosmos [19], Polkadot [20], and Overledger [21], have been launched to address asset and coin transfers and swaps. These projects were deployed because asset or coin transfers can only be achieved through interoperability. They aim to advance cross-industry blockchain technologies for enterprise use cases.

In 2016, the Linux Foundation launched the Hyperledger project with 30 founding members to advance cross-industry blockchain technologies for enterprise use cases. The objective was to create an open-source framework for building distributed ledger solutions beyond cryptocurrencies. The Hyperledger project facilitated enterprise-wide usage of blockchain, particularly for private, secure, permissioned networks. This initiative also prompted discussions on interoperability projects for industry and enterprise use, which will be discussed in this article. The scope of this literature review primarily focuses on cases of blockchain interoperability that apply to enterprises and their relevance to future telecom requirements. This focus eliminates the concentration on cryptocurrency-based permissionless use cases that are less relevant to enterprise applications. As industries undergo digitalization and enterprises experience digital transformation, blockchain technologies, and

 doi:10.20944/preprints202501.2195.v1



interoperable blockchain architecture frameworks can address several industry challenges. Before discussing the details of interoperability, it is necessary to explore how it can reshape the telecommunications industry and what benefits it can add.

## 2. Understanding Cross-Chain Requirements in Telecommunications

In the telecommunications industry, there is a growing need to enable seamless, secure, and tamper-proof transactions for decentralized decision-making and data exchanges between service providers. A straightforward way to address this need is using blockchain and cross-chain communications. However, achieving this cross-chain communication in the telecommunications infrastructure brings challenges, including technical complexities, particularly interoperability, scalability issues, and regulatory hurdles to data privacy and security. According to Jabbar et al. [22], to address these challenges, telecommunications companies and blockchain developers need to collaborate and establish common standards for interoperability. High-quality surveys, literature reviews, and design principles are critical for developing these standards. Furthermore, implementing interoperability for telecommunications requires addressing data fragmentation, reliable provenance, and diverse protocol regulations across different distributions and processes. To address and overcome these challenges, it is essential to identify which telecom use cases best suit blockchain interoperability.

### *2.1. Blockchain Interoperability Use Cases In Telecommunications*

Telecommunications, a heavily regulated sector with high-performance expectations, is still in the early stages of realizing use cases for blockchain interoperability. One critical benefit of blockchain and its interoperability needs is its ability to make decentralized decisions. Below are the predominant applications within the research domain require decentralized decision-making processes.

#### 2.1.1. Identity Management

Due to stringent regulatory and privacy requirements, telecom operators must ensure user privacy and security. Therefore, telecom companies are actively exploring blockchain-based identity management solutions. These solutions are anticipated to enhance security and privacy while enabling secure interoperability among various telecom service providers. According to [23], cloud-based cognitive networks require more comprehensive identity management when users seek access to multiple operators. By implementing dynamic spectrum allocation in next-generation 5G and 6G networks, secure identity management enabling seamless switching between different spectrums is a requirement. Using secure, immutable blockchain technologies enables telecom operators to empower users to maintain control over their identity data and streamline authentication processes across various telecom networks. This authentication process requires a secure data exchange between the operators. Given the regulatory restrictions, whether two or more independent telecom operators can join a single blockchain network and share the same infrastructure is a valid discussion point. Consequently, implementing one identity solution for multiple networks and consolidating operator user bases into a single platform presents significant regulatory challenges. Due to strict regulatory requirements and data privacy rules like the General Data Protection Regulation (GDPR) in the European Union, telecom operators are forced to implement isolated blockchain networks. Secure data exchange layers (cross-chain communication) that provide interoperability with other networks are potential candidates to overcome this challenge. Such an architectural approach can be a standard deployment model for telecom use cases. Once such a secure architecture is deployed, decentralized decision-making can be enabled for many telecommunications use cases, satisfying regulatory hurdles.

#### 2.1.2. 6th Generation Mobile Networks

 doi:10.20944/preprints202501.2195.v1



As 6G evolves, many research papers and surveys, such as [24] and [26], have addressed the new opportunities blockchain technologies provide. A comprehensive survey by Saravanan et al. [23] demonstrated the essential use cases, technical aspects, and challenges of blockchain technologies for 6G technology. Saravanan et al. discussed the challenges of deploying blockchain technologies, including their interoperability. According to [23], interoperability is frequently mentioned as a challenge and an open discussion topic for telecom use cases. According to [24], using blockchain for 3D networking in 6G can provide decentralized and secure data access, offloading, and interoperability solutions. In 6G, global coverage is a significant feature of cellular network connectivity. Based on the initial requirements [25] of 6th-generation mobile networks, three-dimensional (3D) global coverage is deployed. The international communication coverage in 6G concerns the presence of air, space, underground space, and sea. Such coverage requires continuous interaction and strictly controlled access requirements between the layers and other networks. In this sense, smart contracts, distributed ledger technologies, secure identity management, and interoperability introduced by the blockchain are strong candidates. These technical requirements are significant features that allow seamless 6G access and coverage [24]. They also facilitate further use cases such as Industry 5.0, Smart Healthcare, Unmanned Aerial Vehicle (UAV) Applications, Connected Autonomous Vehicles (CAV), Energy Internet, Extended Reality (XR), Holographic Telepresence, and Smart Cities.

Figure 2 demonstrates the 6G SAGIN [28] (space-air-ground integrated network) architecture, which is expected to be deployed in 6G mobile networks by 2030. [27] discussed future directions, opportunities, and challenges for deploying seamless, integrated, and converged architectures. The following sections show how blockchain interoperability can be deployed with SAGIN architectures.

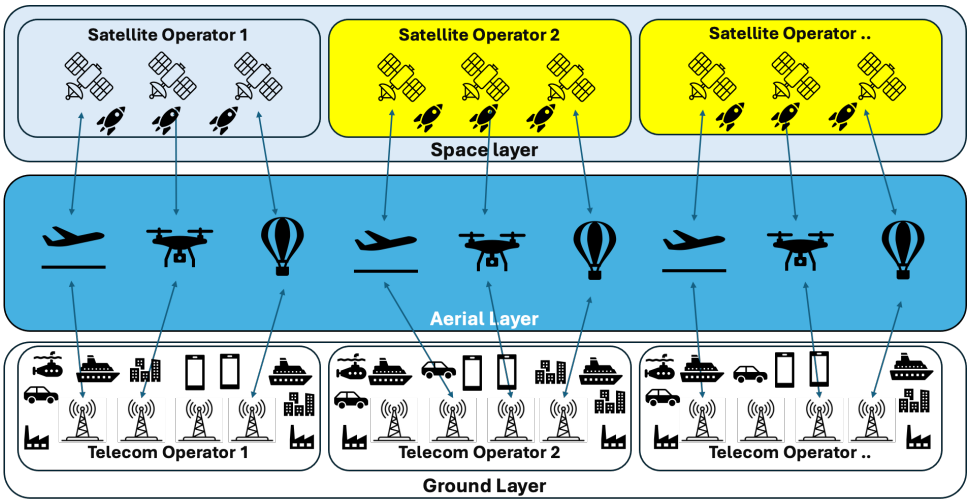



**Figure 2.** th Generation SAGIN Architecture [28].

### 2.1.3. Roaming Services

Roaming services have become a critical requirement in deploying mobile communication services. If a roaming agreement is signed between the home country and the mobile operators of the visiting country, mobile users can enjoy mobile services while visiting a foreign country. Based on roaming agreements, a visitor's use of services and usage records are submitted to a clearing house, an intermediary between the operators. In this process, the clearing house applies processing and settlement fees, resulting in higher costs for the end users. Figure 3 illustrates the international roaming between the two mobile operators in current mobile networks.

 doi:10.20944/preprints202501.2195.v1



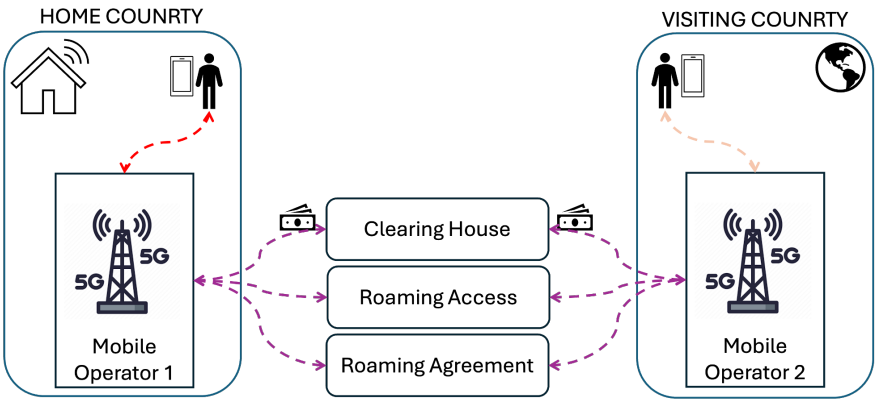



**Figure 3.** International Roaming for Mobile Networks.

Decentralized interoperable blockchain platforms can optimize roaming services by providing transparent, intermediary-free, real-time settlement mechanisms between telecom operators. A candidate blockchain solution can use Smart Contracts as preset roaming exchange rules and automatically apply the process if a roaming service is triggered in the visiting country. Finally, it calculates the roaming fees without an intermediary, such as a roaming-clearing house. Salah et al. [29] discussed roaming as an opportunity in 5G, which blockchain can address. Salah et al. discussed international and national roaming, in which blockchain can improve the quality and experience of roaming services. According to Salah et al., blockchain helps reduce costs and fraud, improves billing accuracy, and enhances the overall user experience of international and national customers. The Global System for Mobile Communications Association (GSMA) [31] has already developed the "GSMA eBusiness Network" [30], using a private, permissioned, industry-wide blockchain network. This blockchain solution focuses on wholesale roaming, clearing, and settlement as the industry's first application. With the introduction of the 6G SAGIN architecture, roaming services are expected to become more complicated and subject to privacy leakage if privacy and identity requirements are not considered. According to [24], roaming fraud is expected in 6G networks due to increased complexity and interoperability requirements.

### 2.1.4. Mobile Number Portability

Mobile Number Portability (MNP) is primarily deployed with intermediaries, such as roaming. For existing 5G and previous generation networks, a clearing house is an intermediary in each country, where MNP is deployed as a semi-automated or fully automated process. Once regulatory requirements have been established, such a process can be efficiently designed using smart contracts as a self-executing autonomous process. Blockchain can easily facilitate number portability by enabling the secure and efficient transfer of phone numbers between different telecom operators using smart contracts and distributed immutable ledgers provided by blockchain technologies. With the addition of interoperability features, blockchain networks can ensure seamless porting processes while maintaining data integrity and security. In [32], Krishnaswamy et al. offered an MNP solution using a permissioned private blockchain based on Hyperledger and Smart Contracts. According to [32], automated, immutable processes with Smart Contracts increase trust, reduce MNP processing time, and eliminate processing errors with a transparent, fully automated, and distributed process. The traditional mobile number portability process is illustrated in Figure 4.

 doi:10.20944/preprints202501.2195.v1



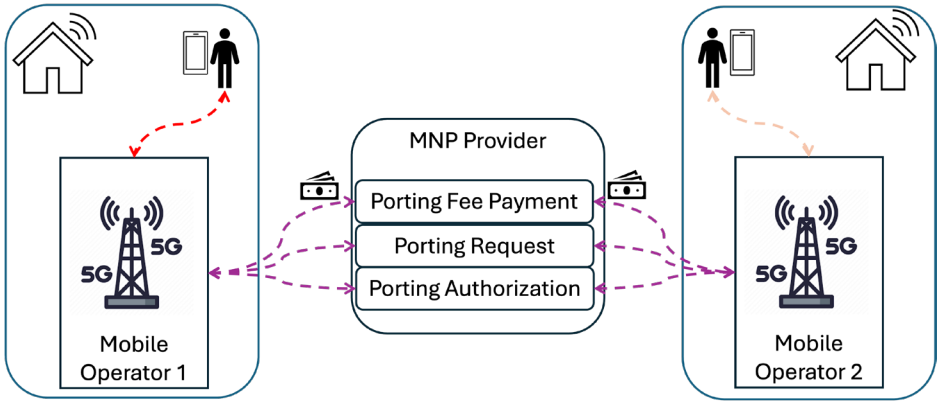



**Figure 4.** Mobile Number Portability Process.

2.1.5. Supply Chain Management

According to [33], dynamic customer needs for existing and new services force telecom operators to manage and track their existing supply chains more effectively. In this respect, Li et al. claimed that well-known features such as decentralization and openness in data tracking and management are clear benefits of using blockchain in supply chain tracking. According to Li et al., when blockchain is used for supply chain tracking, it offers a tamper-proof architecture. Li et al. proposed utilizing blockchain for comprehensive supply tracking and management when implementing the process across multiple vendors and suppliers, including financing and logistics companies. Once the entire process is executed and tracked in the blockchain, it can be considered reliable proof of its existence. Telecom companies can leverage blockchain interoperability to manage their supply chains more efficiently by connecting to other blockchain networks outside their organizations. By integrating blockchain networks among vendors and partners, telecom firms can enhance the transparency, traceability, and efficiency of supply chain process accountability.

2.1.6. Sharing And Monetization

According to a Deloitte Insights report [34], telecom companies have a unique position in managing the relationship between content and customers. Third parties provide most of the content offered to telecom networks. This enhances the creation and provision of new content by third parties. This surge in content creation poses challenges for telecom service providers as they consistently strive to maintain a stable network. The new requirements introduced by the new content can be challenging to manage, as they aim to avoid frequently introducing new features in a stable telecom environment network. Blockchain can effectively manage all existing and new requirements, with a process flow built using Smart Contracts and an autonomous consensus mechanism. Blockchain interoperability has a high potential to enable telecom operators to share and monetize their data assets securely with third-party service providers, advertisers, and researchers. In this view, interoperable blockchain platforms guarantee data privacy, integrity, and consent management while enabling seamless data exchange across networks and third-party content providers.

2.1.7. End-To-End Orchestration Of 6G 3d Wireless Networks

According to [26], end-to-end orchestration in next-generation telecom networks is crucial due to the heightened expectations for low latency and seamless connectivity among multiple service providers. Low latency is a primary feature of 5G and is anticipated to become even more significant among the various endpoints associated with different service providers in 6G. The seamless connectivity in the 6G scenario requires an autonomous and fully automated process. Transparency and traceability of such **processes** are necessary for fine-grained access policies. In this case, with an

 doi:10.20944/preprints202501.2195.v1



integrated interoperability architecture, the blockchain can provide essential requirements and ideal tracing capabilities.

## 3. Benefits of Blockchain Interoperability in Telecommunications

The following benefits can be considered as the most critical:

- **Enhanced security**: Blockchain technology can provide a secure platform for telecommunication transactions by encrypting data and ensuring their integrity through a temper-proof hashing mechanism.
- **Improved interoperability**: Blockchain technology allows seamless data transfer and communication between telecommunication networks, enabling better integration and collaboration among service providers with decentralized decision-making using smart contracts.
- **High transparency**: Integrated distributed ledger technologies make all transactions traceable and transparent to the parties involved when necessary.
- **Increased operational efficiency**: Blockchain technology can streamline and automate telecom processes, including supply chain management, by reducing manual intervention and improving operational efficiency.
- **Cost efficiency**: Blockchain technology can lower costs for telecommunication providers and their end users by eliminating the need for intermediaries and reducing transactional friction.
- **Enhanced customer experience**: Blockchain interoperability can enable seamless roaming services for customers, allowing them to connect to different networks, particularly 6G 3D communications, without disruptions or complicated billing processes.
- Facilitated billing and settlement: Blockchain technology with immutable and fully transparent features can enable more efficient and accurate billing and settlement processes in the telecommunication sector, thereby reducing disputes and delays.

### *3.1. Challenges And Risks of Blockchain Interoperability in Telecommunications*

Despite their potential benefits, there are challenges and risks associated with blockchain deployment in telecommunications. According to [24], six significant challenges can be introduced using blockchain-based solutions: scalability, measurement of decentrality, security and privacy, consensus algorithms, standards, policies, legal issues, and interoperability in deploying blockchain in 6G networks. According to the existing literature, interoperability has the following subchallenges:

- **Technical complexity**: Implementing interoperability across multiple blockchain networks requires technical expertise and compatibility among protocols, blockchain networks, and consensus algorithms.
- **User Privacy & Separated Identity Management:** When two or more standalone blockchain networks are expected to interoperate, their user identities in each network will remain private and undiscoverable by other interoperated networks.
- **Scalability:** Blockchain networks, particularly public permissionless blockchains such as Bitcoin and Ethereum, already face scalability issues with a high volume of transactions. Such problems can also occur in the telecommunications industry even if permissioned blockchains are used. Implementing blockchain interoperability in the telecommunications industry is a complex task requiring technical expertise and compatibility between different protocols and consensus algorithms. It involves collaboration between multiple service providers and establishing common standards to ensure seamless integration and communication; however, it can introduce performance and scalability issues. Using homogenous blockchains in interoperation has a high potential for addressing performance and fewer scalability issues.
- **Regulatory challenges**: Blockchain technology in the telecommunications sector may face regulatory hurdles as it involves exchanging and storing sensitive customer data. Implementing blockchain interoperability in the telecommunications sector requires collaboration among service providers to establish common standards and overcome regulatory challenges

 doi:10.20944/preprints202501.2195.v1



surrounding data privacy and security. With the regulating body, telecom operators might need help with the planned blockchain-based interoperability deployment requirements. In addition to its technical challenges, telecom sector leaders are expected to address regulatory issues by cooperating with regulatory bodies.

Considering these advantages and challenges, it is crucial to carefully choose the most suitable blockchain and interoperability solutions to effectively address a wide range of telecommunications scenarios, particularly in the context of 6th-generation mobile networks. Given the telecom sector's emphasis on robust privacy and security measures, permissionless and public blockchain solutions do not apply to telecom. Therefore, this study explores private and permissioned solutions and strategies. The following section undertakes a comprehensive review of the carefully selected literature to identify and evaluate ideal interoperability solutions and compare them to determine the most suitable candidates.

## 4. Methods And Material

This study focuses on the current 5G and upcoming 6G requirements outlined in widely cited research papers, where blockchain technologies are expected to play a crucial role in the future. Based on these requirements, interoperability is one of the most essential factors for connectivity in 6G three-dimensional networks. These flexible 3D connections enable users to connect seamlessly with air, space, and aerial service providers. Blockchain interoperability can effectively address multilevel interconnections. Previous research, including projects based on permissionless cryptocurrency solutions, has shown that such approaches are unsuitable for enterprise domains due to high security and privacy expectations. The telecommunications domain is even more stringent owing to intense regulatory requirements. Therefore, this study focuses solely on solutions suitable for telecoms within the permissioned blockchain space and explicitly does not aim to provide comprehensive coverage of the literature, as there is already extensive research on interoperability and its coverage.

In contrast, this study selects the most popular and highly cited papers and literature covering these solutions, along with projects developed by well-known organizations, such as International Business Machines (IBM). It covers the most critical design categories and architectural approaches from these projects, research papers, and the literature. The scope of this study enables us to demonstrate research directions for the most substantial and suitable solutions using these categories and architectural approaches, including research directions for the ideal architecture, particularly for 6G communications. Finally, the carefully selected and reviewed solutions were compared to finalize the review and provide research directions by selecting the most suitable solution. Finally, the chosen solution is verified to determine whether it meets the expected criteria for an ideal permissioned interoperability solution. The researchers reading this paper should consider this selection as a guide for future research on blockchain interoperability in telecommunications.

## 5. Literature Review

This study reviews the most cited research papers by considering the essential features required for ideal interoperability. Zakari et al. [35] published a literature review of the opportunities and challenges of the pharmaceutical industry in applying blockchain technologies. Zakari et al. discussed five opportunities blockchain technologies offer: transparency, reduced transaction time, security, cost efficiency, and irreversible transactions. In [35], five primary challenges associated with current blockchain technologies were identified, emphasizing the need for solutions to unlock these opportunities: Interoperability, Scalability, Storage, Social Acceptance, and requires Standardization. These challenges intersect with known issues in the telecom industry, where interoperability is a critical hurdle. Zakari et al. highlighted the importance of security, which is essential for telecom cross-chain communication. Achieving technical interoperability does not eliminate security concerns and remains a complex issue for targeted solutions. In cross-chain communication (CCC), each blockchain enforces separate access policies to maintain privacy and security across different

 doi:10.20944/preprints202501.2195.v1



telecom network operators. This introduces complex security requirements, posing a critical challenge to interoperability. Zamyatin et al. [36] suggested that true interoperability requires a trusted third party, whereas many solutions aim to eliminate the need for intermediaries, aligning with the principle of decentralization.

Blockchain interoperability is a popular topic in supply chain tracking. A pivotal survey by Bellavista et al. [37] examined interoperable blockchains in collaborative manufacturing, which are integral to supply chains. They acknowledged that interoperability remains challenging despite numerous solutions, primarily because of the ongoing security concerns. Bellavista et al. concluded that the design of an interoperability solution must meet high-security expectations. In their survey, Bellavista et al. discussed a security solution called a Trusted Execution Environment (TEE). Using this solution, Bellavista et al. proposed a relay scheme architecture in which information is passed through a relay layer, as shown in Figure 5. Such a TEE deployment with relay architecture is feasible for two interoperated blockchains. However, the implementation can become complex if end-to-end enterprise flow involves more than two blockchains. This could offer security and access rights to all interoperated blockchains. This approach can quickly introduce access policy concerns and conflicts with independent blockchains operating. This is an evident concern for tamper-proof security and the strict access policy requirements in the telecom domain.

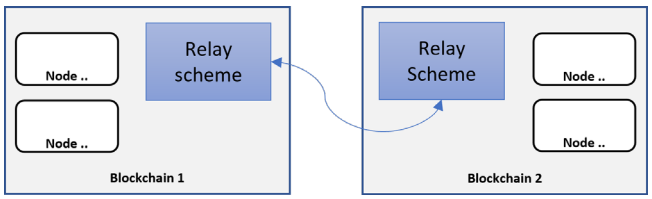



**Figure 5.** Relay Scheme from Bellavista et al. [37].

*5.1. Interoperability Techniques*

Exploring various popular descriptions, use cases, and interoperability techniques in the research field is essential for a better understanding interoperability. According to Belchior et al. [38], interoperability is proposed as "the ability of a source blockchain to change the state of a target blockchain, enabled by cross-chain or cross-blockchain transactions, spanning across a composition of homogeneous or heterogeneous blockchain systems." This definition highlights that even though telecom operators opt for standard and widely used private blockchain solutions, achieving homogeneity in blockchain networks remains challenging. Therefore, an ultimate solution should support diverse types of private blockchain networks.

Ren et al. [39] define blockchain interoperability as "the ability to flexibly transfer assets, share data, and invoke smart contracts across a mix of public, private, and consortium blockchains without any changes to underlying blockchain systems." Ren et al. expand the definition of "ability to change the state of target blockchain" from Belchior et al. with three essential features:

- Asset Transfer
- Smart contract Execution
- Data Sharing

These are the most common types of interoperability. Asset transfers and swapping are the most popular public cryptocurrency-based interoperability solutions. These use cases can also be applied to private blockchains, providing more flexibility in the telecom domain.

Vitalik Buterin, the founder of Ethereum [40], described the general concept of interoperability techniques in 2016. Buterin discussed its three scenarios:

- Centralized or multi-signature notary schemes
- Sidechains/relays
- Hash-locking

 doi:10.20944/preprints202501.2195.v1

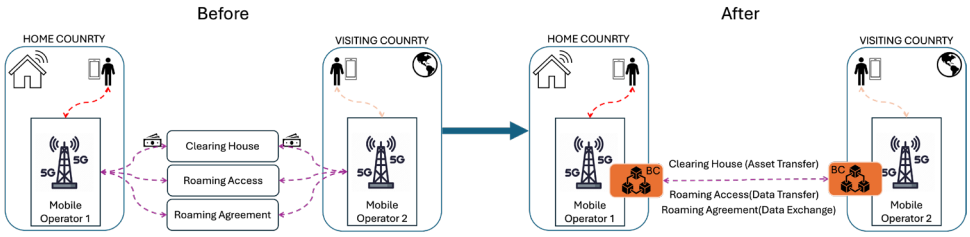


These initial definitions are necessary to explore and expand our understanding of future interoperability schemas. According to Ren et al. [39], in 2023, interoperability techniques were categorized into five schemes:

- **Notary Schemes**: Trusted parties may be considered for centralized and decentralized exchanges. Notary schemes are trendy in cryptocurrency, as there is a high demand for the exchange of cryptocurrency coins worldwide. A famous example is the largest cryptocurrency exchange platform, Binance [41]. The Binance is considered a trusted party when users require currency exchange. Notary schemes, such as trusted intermediaries, are considered centralized solutions and cannot act as candidates for a final solution.
- **Hashed Time Lock Contracts (HTLC)**: Automatically swap currencies for permissionless networks. Unlike notary schemes that require a trusted third party, the HTLC protocol automatically swaps currencies between crypto-coin-based blockchains. There is no intermediary for an HTLC-based solution, which makes HTLC a decentralized solution.
- **Relay Schemes:** execute transactions by replaying transactions among blockchains. They may be trusted or trustless. Trustless schemes agree on the communication protocols between the two blockchains and do not require trustees. If a relay scheme is built as a trusted relay, the solution is an intermediary-based centralized solution. In the final solution, the trustless relay approach is a candidate.
- **Blockchain Agnostic Protocols**: Build an abstraction layer to communicate and interoperate among diverse blockchains. Building an abstraction layer is essential for defining the solution as centralized or decentralized. In 2019, Abebe et al. [42] proposed a relay component that abstracts the existing blockchain modules from the interoperability layer. The architecture presented in [42] is constructed as a decentralized solution without a trustee. It is one of the earliest solutions for permissioned blockchain networks built with Hyperledger [43,44]. The design offered by Abebe et al. also provides a side-by-side architecture and serves as a foundation for future projects at the Hyperledger.
- **Sidechains**: transfer assets from the main chain to the side chain. Consequently, the side chain transfers the assets to the final chain. If this intermediary chain is responsible for the interoperability of two independent blockchains, the challenge lies in who owns the side chain and how it is managed. Therefore, sidechains cannot act as a decentralized interoperability approach when deployed as intermediaries between interoperating blockchains. In the final solution, a sidechain can still be used if it is deployed as a side component of that chain and does not act as an intermediary.

As previously mentioned, these five schemes focus on the interoperability of the two chains. When a third or more interoperated blockchains are involved, the process becomes more complex in an end-to-end enterprise process that spans multiple chains. This scenario type is called Blockchain of Blockchains (BoB) by Belchior et al. [38]. In Figure 5, you can see the illustration of an international roaming use case where a decentralized, intermediary-free process is developed with blockchain interoperability. Once blockchain networks are formed for the interoperation between multiple telecom operators, this can be described as a BoB.

Figure 6 illustrates how future telecoms can form interoperable processes with other telecom operators. Blockchain interoperability cases were also applicable to 6G. Figure 6 illustrates how different parties are integrated with the 3D 6G space for future telecom interoperation landscapes.



 doi:10.20944/preprints202501.2195.v1



**Figure 6.** A Blockchain Interoperability for International Roaming.

Figure 7 illustrates the mobile number portability process for the three mobile operators. Once the MNP provider shown in Figure 4 is eliminated and handled as a decentralized process with no intermediary, the blockchain layers form a process between the three mobile operators.

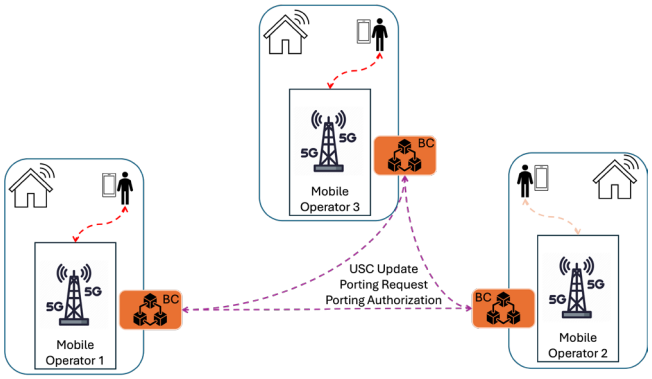



**Figure 7.** Mobile Number Portability Process with Blockchain.

For 5G and 6G networks, a decentralized MNP process can be established using interoperability layers. When a user triggers a porting request, the blockchain network sends the request to the target mobile subscriber. Suppose the user ports from Network 1 to Network 2, and the Unique Subscriber Code (USC) is transferred to the target operator. Once the porting request is completed, asset exchange occurs from the blockchain perspective. Consequently, the new owner of USC is shared with Operator 3. This is considered data sharing from a blockchain perspective, and an update is reflected in the blockchain's distributed ledger.

*5.2. Future Telecom Use Cases with Blockchain Interoperability*

Figure 8 shows two telecom providers with three blockchains deployed in their infrastructure. Each of these blockchains interacts with third parties or service providers. Based on the initial use cases, blockchain interoperability can be achieved in the following scenarios:

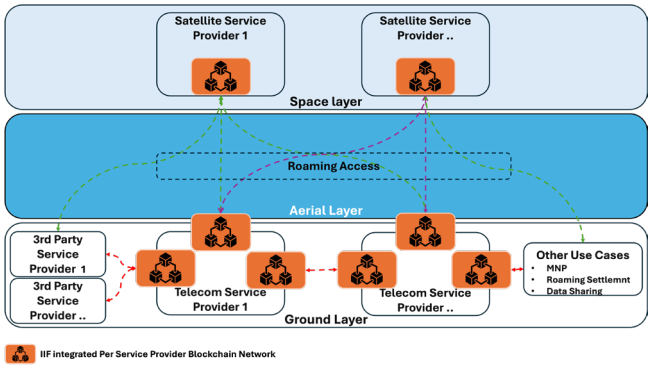



**Figure 8.** Blockchain Interoperability Architecture for 6G.

- **National/International Roaming Access**: Under agreed-upon conditions, a telecom service provider can connect to another national/international service/telecom provider, allowing users to use their roaming services seamlessly. Figure 5 illustrates this process.
- Roaming Payment Settlement: Without a roaming clearinghouse(intermediary), telecom providers can agree to pay to visit customers' roaming records and settle payments directly with interoperating telecom providers.

 doi:10.20944/preprints202501.2195.v1



- **Mobile Number Portability (MNP)**: This can be introduced in countries where multiple telecom providers offer services, and users can port their services to other operators. However, this process currently trusts intermediaries managing the end-to-end process, causing delays. 6G is expected to offer broader services than 4G and 5G. Using 6G with new-generation mobile phones with eSIM(embedded SIM) capabilities can boost the need for MNP with almost no operational difficulties. Once blockchain interoperability is deployed in each operator, the layer can eliminate the intermediaries and accelerate the end-to-end process. The new process is illustrated in Figure 6.
- **Third-Party Services Access & Payment Settlement**: Telecom operators use third-party content services. Blockchain interoperability can automate access to such services and content. Third parties can access operators' blockchain layers to offer services, and payments can be made automatically using blockchain interoperability layers.

*5.3. Essential Design Requirements*

The blockchain-based interoperability architecture can cover the aforementioned use cases for future 6 G telecoms. The essential design requirements for future telecoms are outlined below based on the existing literature and popular projects.

- **Single Point of Failure (SPoF):** According to Bhatia et al. [45], intermediaries such as notary schemes and side chains introduce an SPoF in interoperability designs. In such a design approach, the interoperability of cross-chain communication is not operational when the intermediary decreases. This is a typical SPoF issue because no alternative or backup solution exists.
- **Decentralization**: This is the most famous feature of the blockchain technology. The Blockchain promises to eliminate any authority or intermediary that may rule the interoperability process and make decisions when executing transactions. Atzori [46] discussed government-owned processes and asked whether such intermediary government processes are necessary. [46] claimed that blockchain technology is the most famous feature of blockchain technology. [46] asserts that blockchain technologies represent a disintermediation process that can remove intermediary state-owned processes. Atzori even addresses the state or governing authorities, causing a single point of failure (SPoF), as they cannot respond to the rapidly changing needs of society and face scalability challenges in delivering services. According to Chen et al. [47], decentralized enterprise models create new opportunities. Similarly, Zheng et al. [48] indicated that blockchain cryptocurrencies' existing mining consensus models allow large miners to dominate the mining process. Both studies suggested that centralized architectures or models should be eliminated.
- **Safety of Access Management & Policies**: Every independent permissioned blockchain has specific user-access management rules and policies. The rules, such as consensus mechanisms and executed smart contract-based rules, are particular to the blockchain network. When an interoperability architecture is offered, there is an expected tendency to synchronize and unify both blockchains' access management. Dagher et al. [49] proposed a framework that preserves patient privacy in a national health system while using blockchain to manage private patient data access. According to Dagher et al., patient data confidentiality must be maintained if external access is required. Ren et al. [39] stated that the user identity and data can be detected when a trusted intermediary is used for interoperability. Therefore, intermediaries should be prevented, and trustless decentralized approaches should be chosen to keep users' identities safe.
- **Sovereignty**: In contrast to these approaches, Ghosh et al. [50] provided a cross-network identity framework that manages decentralized identities (DID) in an interoperability network. The self-sovereignty of blockchains in a multi-network architecture allows each blockchain to choose which users and groups can access their DLT from other chains and which functions they can execute through cross-chain communications. Decentralized identities allow users self-

 doi:10.20944/preprints202501.2195.v1



sovereignty. However, unified access management and policies for interoperated blockchains can introduce unexpected access leakages. These statements indicate that the user rights, access policies, and data are preserved and isolated. In such cases, DIDs with minimum user extensions can have a much more secure and minimally affected interoperability.

- **Core Blockchain Process Isolation**: Pongnumkul et al. [51] evaluated the private blockchain performance under various workloads. The results show that the performance of blockchain frameworks still needs to be improved when high workloads are involved, and their processing speeds are not competitive with existing database systems. In their project, Ethereum and Hyperledger Fabric were compared, with Hyperledger Fabric emerging as a clear winner, exhibiting even ten times less latency and much higher processing capacities. These results indicate that performance issues are critical in core blockchain transaction processing. Further performance drawbacks may be introduced when an additional interoperability solution is deployed in the core blockchain network. DApps and Smart Contracts are designed to facilitate the interaction of the blockchain with external applications. Vacca et al. [52] stated that the performance of a DApp is vital for assessing the blockchain efficiency. Therefore, Vacca et al. evaluated the performance of both DApps and Smart Contracts in their research paper. They demonstrated the test results of the DApps and smart contract deployments, which revealed varying performance outcomes. Any additional design framework for the core blockchain must be carefully conceived and tested before its implementation for interoperability. Such a design must also be isolated from the core blockchain process to minimize its impact on performance.
- **Storage of Traceability Transactions**: Once transactions in a traditional blockchain increase, the long-term storage of transactions for traceability needs might become a real challenge. Musungate et al. [53] discussed using DLTs as storage in main blockchain networks that can quickly become large owing to crowded blockchain domains. Traditionally, the main chain has been expected to provide decentralization, intercommunication, security, and privacy. Features such as extensive storage management are focal points in most projects. According to Yadav et al. [54], such significant storage needs can quickly become a performance issue when the main chain is queried frequently for transaction history. Yadav et al.. offered a storage land registry for national health systems frequently queried by doctors and health system users. Musungate and Yadav suggested using a sidechain approach to achieve better performance and storage management, considering the main chain only for the standard blockchain features. In an ideal interoperability design, significant storage needs and high-performance expectations can be addressed using side chains instead of main chain-based approaches.

After conducting a comprehensive literature review, the identified essential design requirements were crucial for developing an optimal blockchain interoperability project for future telecom domains. To achieve this, well-established projects from the existing literature and the research landscape were selected and reviewed to determine whether they could meet these essential design requirements. This approach enables telecom operators to accelerate the design and implementation of blockchain interoperability in the current and future processes.

### *5.4. Review of Well-Known Permissioned Blockchain Interoperability Projects*

Hyperledger Cactus [55] is the Hyperledger Foundation's initial interoperability project. It has been built as a bridge between the Hyperledger Fabric and Ethereum for cross-chain communications. This was one of the earliest solutions implemented as a proof of concept for permissioned blockchains. The cactus was considered a notary. Similar notary solutions built between two interoperated blockchains are classified as centralized solutions and intermediaries. This type of intermediary architecture also introduces a single point of failure when an intermediary is unavailable.

Bradach et al. [56] proposed a gateway-based solution in 2022, where a gateway was used for cross-chain communications between two interoperating blockchains, Hyperledger and Corda. In the gateway part, a router is responsible for routing the message from the hyperledger connector to the

 doi:10.20944/preprints202501.2195.v1



Corda connector. This approach can be considered a cross-chain-trusted relay. Bradach et al. call this solution middleware, which is, by other means, an intermediary. Although such an intermediary solution is deployed outside both chains, it raises the question of who maintains this component. This approach generally breaks down decentralized architectures and presents a centralized solution.

Weaver [57] is a new approach that provides substantial enhancements compared with existing solutions. Weaver is based on Hyperledger Fabric and aims to provide interoperability between Distributed Ledgers (DLTs) of the same or different types of permissioned blockchains. Weaver offers three use cases: data-sharing, asset transfer, and asset exchange. Weaver introduced two modules as side components for each interoperating blockchain. The Intop is responsible for communicating with the core blockchain. A relay is used to communicate with the interoperated blockchain and includes a communication module for each blockchain type, such as Corda, Hyperledger, and Ethereum. Weaver access management modules are currently being developed. Weaver's design is a side-by-side architecture and isolated framework, making it a decentralized solution. Weaver also uses asynchronous and message-based communication between interoperation modules. These two features make the Weaver a more flexible and fault-tolerant solution. The fast and efficient communication protocol gRPC is also used to communicate between interoperated blockchains. The design choices were carefully made and could be essential for an ideal solution. It also aims to deploy DID architecture for identity management. This design allows over two blockchains to interoperate, making Weaver a strong candidate for the final permissioned blockchain interoperability solution.

Hyperledger Firefly [58] is a promising solution for the future of blockchain technologies. This project aims to accelerate the development time for future blockchains, notably by introducing a Web3 development framework. Firefly offers a solution based on the permissioned data passing through multiple chains. According to Kang et al. [59], Firefly requires a third party to validate the nodes, which introduces a security bottleneck. This type of third-party validation also introduces an intermediary that can be considered centralized. Although Firefly provides flexible development environment tools for DApps in Web3, its design architecture is very complex for simple data and asset transfers.

Hermes [60] was proposed by Belchior et al. and concentrates on fault tolerance for possible crash cases of middleware-based interoperability. Hermes aims to achieve a single point of failure-free architecture to eliminate crash-causing cases and provide crash resilience. Hermes presented a valid use case that can be integrated into future designs. However, using a gateway-based intermediary architecture, particularly for fault-tolerant design, renders Hermes a centralized architecture.

Yui [61]: Yui is an incubation project at Hyperledger Labs that provides cross-chain communication for heterogeneous blockchains. It uses the IBC protocol for cross-chain communications and offers a relayer service as middleware. Although the relayer cannot be considered a genuinely trusted party, it still acts as an intermediary module between the two interoperable blockchains. The initial design does not support side-by-side deployment of the modules. However, if a side-by-side approach is applied in the later stages, it can also be considered a strong candidate.

Dinh et al. [62] proposed a design blueprint for interoperable blockchains, focusing on access control, cross-chain transactions, and communication. These three challenges are valid for cross-chain telecommunications. Dinh et al. added access control, transactions, and communication to each side of interoperated blockchains such as Weaver. These three components isolate the core blockchain from the interoperability modules. An interoperability architecture is proposed by Dinh et al. using side-by-side components. The design of Dinh et al. makes the final architecture a decentralized solution using a side-by-side approach and isolated modules. Bellavista et al. [37] offered a similar side-by-side approach. The authors called their design a relay scheme responsible for relaying transactions from one blockchain to another.

### *5.5. Comparison of Interoperability Projects*

 doi:10.20944/preprints202501.2195.v1



The review results covered design issues and an analysis of well-known projects. As a result, an ideal telecom solution was proposed. This solution and approach can be a foundation for the interoperability of existing and future telecom projects. As previously demonstrated, permissioned blockchains include must-have features for future telecom and 6G deployment. Therefore, permissioned blockchains are a critical requirement in telecom use cases. In [63], the proposed initial design principles were presented as supporting research papers. Details of these projects and design approaches are provided in [63]. If required, the readers of this paper can view the design architectures in [63]. Six design principles were covered in [63]: Decentralization, Homogeneous Networks, Smart Contracts, Wide Range of Contributors, Single Point of Failure, and Side-by-Side Architecture. The results combine these design principles with the additional topics covered in this review, such as access management and policies' safety and core blockchain process isolation. Conversely [63], heterogeneous blockchain interoperation is crucial for the enterprise processes formed by blockchain frameworks and telecom use cases.

The review results established eight distinct comparison categories for an ideal blockchain interoperability solution, offering a forward-looking approach to the final design. These categories are defined as follows:

- **Interoperability Type**: Interoperability in blockchain solutions supports various types, such as permissioned, permissionless, or hybrid. Each type of blockchain has its own feature set, which affects security and access policies. These features are crucial in ensuring private blockchain interoperability in the telecom industry. The hybrid type involves a combination of private and public blockchains within a solution.
- **Decentralization**: Current project designs include intermediaries, notaries, and side-by-side modules that facilitate interactions between blockchains. However, these patterns are sometimes decentralized. In the telecommunications field, intermediaries causing centralization should be removed.
- **Multi-Network Support:** Many solutions are tailored to connect two blockchains. Assessing whether a solution is scalable for future research and enterprise endeavors, such as multinetwork integration, is crucial. These solutions should facilitate the interoperability of three or more blockchains, which is becoming increasingly important with the emergence of the 6G technology.
- **Chain Isolation**: Isolating the main chain provides a strict access policy and minimizes external effects. Most solutions offer direct access to a relayer or an intermediary. This approach renders the solution vulnerable to attackers, particularly in the case of regulated telecoms. A thin interoperability layer with multiple layers has a minimal effect on the main chain operation. It protects the solution from external attacks and provides high-level user privacy and security.
- **Sovereignty**: Numerous solutions presented in current research projects provide integrated and synchronized access policies between interconnected blockchains. However, synchronizing access policies can create security vulnerabilities that hackers can exploit. The main chain is expected to remain autonomous and enforce restricted minimal access policies for interoperability solutions without unifying the access policy with interconnected chains. This approach aims to safeguard user privacy and establish self-sovereignty in telecommunication.
- **Storage Efficiency**: In a traditional independent blockchain network, the main chain is expected to be the central storage for status updates in DLTs. For interoperated blockchains, especially 6G, the storage requirement is expected to be much higher because of the additional storage required for interoperability. According to Yang et al. [64], side chains extend the storage capability of blockchains and are a better choice in certain blockchain-use cases. Therefore, managing storage in an inter-operational architecture is critical. According to the test results in [35], a sidechain-based solution eliminates the storage problem of the main chain. The results from [64] also show that when data are separated into main and side chains, access to a separated side chain is much more secure and has less of a performance effect on the main chain.

 doi:10.20944/preprints202501.2195.v1



- **Support Community**: If a larger developer community supports the selected solution and its components, it will have a much longer life cycle and be a strong candidate for future projects. The strength of the support community for integrated blockchain networks and supported solutions is critical.
- **Side-by-Side Design**: Unlike the intermediaries proposed in most solutions, the side-by-side approach in each blockchain network strengthens sovereignty and chain isolation in interoperability.

## 6. Results

The comparison and evaluation results of interoperability solutions are displayed in Table 1. Based on the requirements and essential feature set, researchers can identify the most suitable solution for a specific telecom use case

**Table 1.** Comparison Of Covered Interoperability Solutions.

| | Interoperability | Decentralized | Multi-Network | Main Chain Isolation | Sovereignty | Storage Efficiency | Side-by-side Design | Support Community |
|---|---|---|---|---|---|---|---|---|
| **Cactus [55]** | Hybrid | O | O | O | O | O | O | Medium |
| **Bradach et al. [56]** | Permissioned | O | O | O | O | O | O | Weak |
| **Firefly [58]** | Hybrid | P | P | O | P | O | O | Strong |
| **Hermes[59]** | Permissioned | O | O | O | O | O | O | Weak |
| **Yui[60]** | Hybrid | O | P | O | P | O | O | Medium |
| **Dinh et al.[61}** | Permissioned | P | O | O | O | O | P | Weak |
| **Bellavista et al.[37]** | Permissioned | P | O | P | P | O | P | Weak |
| **Abebe et al.[42]** | Permissioned | P | O | P | P | O | P | Weak |
| **Waever[57]** | Hybrid | P | P | P | P | O | P | Medium |

To align with telecom's strict privacy and security requirements, only permissioned blockchain solutions should be considered for the final interoperability deployment. Decentralization is crucial since intermediaries cannot be part of the final design, especially in telecom. Mainchain isolation is a vital aspect that should be considered for improved performance and security; however, this may not be a high priority for an initial MVP. Sovereignty is also a key deciding factor for privacy expectations and should not be extended to a hybrid access management model. Due to limited literature, a performance design solution can be planned for future research projects, as much of the existing literature has failed to provide solid arguments for this study. A solution supported by a strong community will encourage researchers to invest in a future-oriented design. A side-by-side design is the most critical feature for decentralization and privacy security. The results indicate that Weaver is a comprehensive solution for deploying a private multidomain blockchain architecture. Weaver is also designed as a side-by-side architecture that supports multiple deployments of interoperated chains. The results of this study suggest that the storage efficiency features are critical performance topics.

The Weaver architecture illustrated in Figure 9 was designed for heterogeneous hybrid blockchain networks. Recently, Weaver merged with the Hyperledger Cacti project, which aimed to provide more cross-chain communication options by unifying the existing Cactus project with Weaver. As of January 2025, Weaver's design offers interoperability relays for Hyperledger Fabric, Hyperledger Besu, and R3 Corda, including data transfer, asset transfer, and asset exchange features.

 doi:10.20944/preprints202501.2195.v1



Hyperledger Besu is an Ethereum client designed as an enterprise-friendly blockchain supporting permissionless and permissioned requirements. R3 Corda is designed for financial service interoperability, allowing value exchanges between R3 users. These three projects are popular in research and are supported by a significant community.

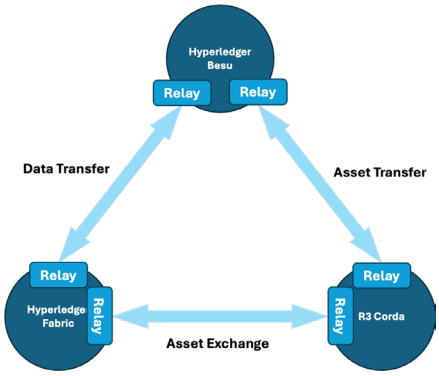



**Figure 9.** Weaver Interoperability Framework.

Due to its extensive feature coverage, Weaver's architecture is a strong candidate for future telecom use cases and 6G roaming/interconnection requirements. Research alternatives have yet to address the requirements for performance and storage needs. 6.1 Contribution To The Research Space

Simultaneously, the insights gained from this study and the proposed research directions ensure this study contributes to the research domain in several ways. The importance of interoperability across multiple blockchain networks, especially in the context of 6G projects, was illustrated by comparing the traditional interoperability between two distinct blockchain networks. The application of the Weaver framework shows the feasibility of integrating two or more blockchain networks, serving any multi-network domain that requires a permissioned interoperability design. Furthermore, the critical role of security in telecommunications is highlighted by demonstrating a side-by-side architecture. This architecture prevents unified access policies, thereby protecting the access layers of the main chain. This is essential for ensuring telecom users' privacy and security while addressing some critical regulatory matters. This discussion also emphasizes the importance of primary chain isolation regarding blockchain interoperability. Since blockchain performance is vital, any extended design proposal must undergo thorough experimentation, mainly when introducing 6G complex interconnection features. Finally, this literature review demonstrates how blockchain's inherent characteristics, such as enhanced transparency and traceability, play a crucial role in interoperability and interconnection within telecommunications 6th Generation 3D mobile networks. As the 6G 3D network incorporates complex access policies, robust access management tasks will be introduced exponentially. When a unified access management strategy is implemented, this can reveal vulnerabilities to cyber-attacks. This study demonstrated that a side-by-side approach makes it feasible to avert cyber-attacks and establish a tamper-proof architectural framework, thereby ensuring end-to-end traceability and transparency.

## 7. Research Challenges, Future Directions

The findings from this study have outlined potential avenues for current and future applications of blockchain technology in the telecommunications sector. The analysis suggests that the Weaver framework has emerged as a high-potential model for future research. Weaver's unique design, characterized by its isolated structure, is projected to reduce the impact on interoperability and traceability performance significantly. To proceed with further research, it is essential to understand the key challenges concerning interoperability that could impact the successful implementation of Weaver in the telecom research area.

 doi:10.20944/preprints202501.2195.v1



*7.1. Deployment Challenges*

Weaver's high potential presents a couple of challenges. Weaver is currently under development, and some critical features still require discussion. Here are the essential topics that must be considered for successful deployment:

- **Scalability**: The history of blockchain technology is full of performance issues and discussions. As discussed in the previous sections, new blockchain projects have been designed to address scalability and performance limitations, particularly in public blockchain research. 6G communications with seamless transitions between interoperated telecom operators require strong performance due to the ongoing transaction processing for service access and usage tracking. According to [69], 6G requires an increasing demand for higher capabilities and broader spectrum communications of mobile technologies. According to [68], once the Distributed Metaverse[68] is deployed in mobile networks, such an architecture requires higher scalability and capability. Gadekallu et al. [70] also discussed performance as a challenge for blockchain for edge-of-things (BEoT) devices deployed in 5G networks when the number of edge devices increases significantly. Therefore, Gadekallu et al. suggested moving algorithms to edge devices to minimize data travel between data centers and edge devices. Such a scenario will become more challenging when these BEoT devices travel between 6G networks.
- **Storage Management**: Once the transaction processing per planned time frame increases significantly, storing these transactions on the mainchain can become a challenge and performance bottleneck for end-to-end transaction storing and traceability. In [71], Xie, Junfeng, et al. surveyed the scalability of blockchain systems. According to [71], traditional blockchain nodes deployed for enterprise use require more storage space. If this issue is not addressed, it could lead to transactional delays as network density increases. In [72,73], off-site solutions were explored as alternatives to improve performance and manage storage more efficiently. [72] also examined the TEE solution by Bellavista [37] et al. as an off-chain option. This challenge necessitates further research into off-chain solutions, including sidechain options, as suggested in this study.
- **Regulatory Hurdles**: Despite various alternative interoperability solutions, regulatory bodies may permit information exchange between telecom providers only if an intermediary is utilized. In many countries, regulatory bodies designate official intermediaries for information exchange, as regulations and processes are necessary. Therefore, regulatory bodies must develop and implement new regulations for a direct peer-to-peer information exchange framework managed by a potential interoperability solution.

*7.2. Future Directions*

It is essential to focus on maintaining the three critical aspects of blockchain technology: decentralization, which spreads control across multiple locations or entities by eliminating intermediaries; immutability, which ensures that once information is added, it cannot be altered; and transparency, which allows for the clear visibility of transactions. This literature review highlights four additional areas for future research and discusses why they must be focused on:

- **Side-by-Side Architectures:** Weaver offers a side-by-side architecture that eliminates intermediaries. Future research on Weaver and similar approaches should be continued by observing future developments in such projects. Any new solutions are also expected to provide a side-by-side architecture to avoid intermediaries and centralized processes.
- **High Security-Oriented Approaches**: Interoperability solutions risk introducing vulnerabilities when interoperated blockchain networks are combined with restricted access and privacy policies. Weaver's thin integration layer eliminates such a merge and provides an ideal approach for enhancing security. However, any new design approach must be evaluated to determine whether it aligns with the strict access and privacy policy requirements.
- **Isolated Mainchain**: According to [64], there are three main advantages when a main chain is isolated and integrated with a sidechain. A side chain can be used to store and process high-

 doi:10.20944/preprints202501.2195.v1



transaction-requirement use cases. It can also provide more space for transaction storage, faster data access, and higher security. The project for which the sidechain offered in [64] was conducted to safeguard customer privacy regarding medical information in the health sector. Such a solution designed for customer privacy can also be applicable in telecom. A popular review paper [74] deeply analyzes existing sidechain solutions built for permissionless networks. [74] examines four well-known sidechain solutions, including Loom [75]. This review paper can be considered for future sidechain research. According to [76], smart contracts are essential for deploying sidechain solutions. A smart contract-based layer must be developed and deployed if the main chain needs integration with the side chain. When further sidechain solutions such as [73,77] are analyzed, it is evident that they use permissionless or cryptocurrency-based solutions such as Ethereum, Ardor, or Loom, which lack strict privacy features. This concludes that more research is required on privately permissioned network-based sidechains. The solution in [78] integrates a sidechain with the mainchain using a Cross-Chain Smart Contract (CCSC) architecture. Interoperable networks must consider using smart contracts once the interoperability between heterogeneous networks is required. Considering the existing literature, this research area might bring potential advantages, especially for 5G and 6G interoperability that require higher performance and security.

- **Scalable Architectures**: As suggested in this study's final approach, scalable architectures like sidechains need further analysis to determine their potential for contributing to the research space. [73] presents a sidechain approach to enhance efficiency and speed up transaction processing for 5G use cases. Most sidechain solutions aim to improve the main chain's performance by minimizing interactions outside the blockchain network. This method is crucial for future research, and the selected requirements must retain the advantages of private blockchain architectures for an ideal interoperability framework.

## 8. Conclusions

Blockchain interoperability remains a prominent area of future research, particularly in the telecommunications industry. It can significantly improve various aspects of telecommunications infrastructure, especially in the context of the existing 5G and anticipated 6G 3D SAGIN design. The combination of blockchain and its interoperability features is expected to provide significant benefits, including flexibility, immutability, security, efficiency, and transparency. Closely monitoring blockchain interoperability research is crucial for fully leveraging these advantages. Numerous interoperability projects are currently available and continuously expanding, particularly in the permissioned blockchain research area. The existing research is minimal and has not yet reached a universally applicable level. Based on the ongoing research and literature review findings, more time is required to develop a comprehensive solution for telecom interoperability. The emergence of the metaverse is also a significant driver as it aims to establish a fully decentralized architecture. This will also be integrated into a telecom service provider network once deployed. The interoperability of permissioned and permissionless networks is essential in Metaverse[68], making it a crucial focus for new and ongoing research projects. The results presented here have identified potential research directions for telecom interoperability and highlighted essential design considerations as new research areas, allowing researchers to approach the topic from a broader perspective.

## References

1. Nihham, Solmaz, et al. Intelligent O-RAN for beyond 5G and 6G wireless networks. In: IEEE Globecom Workshops (GC Wkshps). IEEE, 2022. p. 215-220.
2. YANG, Mao, et al. OpenRAN: a software-defined ran architecture via virtualization. ACM Sigcomm computer communication review, 2013, 43.4: 549-550.
3. O-RAN Alliance https://www.o-ran.org/

 doi:10.20944/preprints202501.2195.v1




4. Gkagkas, Georgios, et al. "The Advantage of the 5G Network for Enhancing the Internet of Things and the Evolution of the 6G Network." Sensors 24.8 (2024): 2455.
5. Dangi, Ramraj, et al. "6G Mobile Networks: Key Technologies, Directions, and Advances." Telecom. Vol. 4. No. 4. MDPI, 2023.
6. Cuellar, David, Muntadher Sallal, and Christopher Williams. "BSM-6G: Blockchain-Based Dynamic Spectrum Management for 6G Networks: Addressing Interoperability and Scalability." IEEE Access (2024)..
7. Pasdar, Amirmohammad, Young Choon Lee, and Zhongli Dong. "Connect API with blockchain: A survey on blockchain oracle implementation." ACM Computing Surveys 55.10 (2023): 1-39.
8. Ezzat, Shahinaz Kamal, Yasmine NM Saleh, and Ayman A. Abdel-Hamid. "Blockchain oracles: State-of-the-art and research directions." IEEE Access 10 (2022): 67551-67572.
9. Park, Andrew, et al. Interoperability: Our exciting and terrifying Web3 future. Business Horizons, 2023, A Survey on the Use of Blockchain for Future 6G:Technical Aspects, Use Cases, Challenges and Research Directions.4: 529-541.
10. Qin, Rui, et al. Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 53.4: 2073-2082.
11. Metaverse, https://en.wikipedia.org/wiki/Metaverse
12. Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4(2), 15.f
13. Buterin, V. (2013). Ethereum white paper. GitHub repository, 1, 22-23.
14. M. Conti, E. Sandeep Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416-3452, Fourthquarter 2018, doi: 10.1109/COMST.2018.2842460.
15. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1
16. Raval, S. (2016). Decentralized applications: harnessing Bitcoin's blockchain technology. " O'Reilly Media, Inc.".
17. Yakovenko, A. (2018). Solana: A new architecture for a high-performance blockchain v0. 8.13. Whitepaper.
18. Adam Hayes Investopedia, What is a Blockchain? https://archive.md/7oXqO Kwon, J., & Buchman, E. (2019).
19. Cosmos whitepaper. A Netw. Distrib. Ledgers, 27.
20. Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White paper, 21(2327), 4662.
21. Verdian, G., Tasca, P., Paterson, C., & Mondelli, G. (2018). Quant overledger whitepaper. Release V0, 1, 31
22. Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B., & Raza, U. (2020, November 20). Blockchain-enabled supply chain: analysis, challenges, and future directions. https://doi.org/10.1007/s00530-020-00687-0
23. Raju, S., Boddepalli, S., Gampa, S., Yan, Q., & Deogun, J. S. (2017, May). Identity management using blockchain for cognitive cellular networks. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
24. Kalla, Anshuman, et al. "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions." Journal of Industrial Information Integration 30 (2022): 100404.
25. M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," IEEE Open Journal of the Communications Society, vol. 1, pp. 957–975, 2020.
26. Tataria, H., Shafi, M., Molisch, A. F., Dohler, M., Sjöland, H., & Tufvesson, F. (2021). 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. Proceedings of the IEEE, 109(7), 1166-1199.
27. Ray, P. P. (2022). A review on 6G for space-air-ground integrated network: Key enablers, open challenges, and future direction. Journal of King Saud University-Computer and Information Sciences, 34(9), 6949-6976.
28. Cui, H., Zhang, J., Geng, Y., Xiao, Z., Sun, T., Zhang, N., ... & Cao, X. (2022). Space-air-ground integrated network (SAGIN) for 6G: Requirements, architecture and challenges. China Communications, 19(2), 90-108.

29. Chaer, A., Salah, K., Lima, C., Ray, P. P., & Sheltami, T. (2019, December). Blockchain for 5G: Opportunities and challenges. In 2019 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.
30. GSMA, "GSMA eBusiness network," GSMA, 2022 https://www.gsma.com/services/gsma- ebusiness-network/
31. Global System for Mobile Communications Association www.gsma.com
32. D. Krishnaswamy et al., "The Design of a Mobile Number Portability System on a Permissioned Private Blockchain Platform," 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 90-94, doi: 10.1109/BLOC.2019.8751231.
33. LI, Huidi, et al. Blockchain technology empowers telecom network operation. China Communications, 2022, 19.1: 274-283.
34. Arkenberg, Chris, et al. How can telecom, media, and entertainment find value in blockchain? Deloitte Insights, 2018, 1-14.
35. Nazik Zakari, Muna Al Razgan, Amai Alsaadi, Haya Alshareef, Heba Alsaigh, Lamia Alashaikh, Mala Alharbi, Rana Alomar, Seham Alotaibi, Blockchain technology in the pharmaceutical industry: a systematic review, DOI 10.7717/peerj-cs.840
36. Zamyatin, Alexei, et al. "Sok: Communication across distributed ledgers." Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II 25. Springer Berlin Heidelberg, 2021.
37. Bellavista, P., Esposito, C., Foschini, L., Giannelli, C., Mazzocca, N., & Montanari, R. (2021). Interoperable blockchains for highly integrated supply chains in collaborative manufacturing. Sensors, 21(15), 4955.
38. Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. ACM Computing Surveys (CSUR), 54(8), 1-41.
39. [39] Kunpeng Ren, Nhut-Minh-Ho, Dumitrel Loghi, Interoperability in Blockchain: A Survey, DOI:10.1109/TKDE.2023.3275220
40. Buterin, V. (2016). Chain interoperability. R3 research paper, 9, 1-25.
41. Binance, www.binance.com
42. Abebe, E., Behl, D., Govindarajan, C., Hu, Y., Karunamoorthy, D., Novotny, P., ... & Vecchiola, C. (2019, December). Enabling enterprise blockchain interoperability with trusted data transfer (industry track). In Proceedings of the 20th international middleware conference industrial track (pp. 29-35)
43. Hyperledger Fabric, https://www.hyperledger.org/projects/fabric
44. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15
45. Bhatia, R. (2020, October). Interoperability solutions for blockchain. In 2020 international conference on smart technologies in computing, electrical and electronics (ICSTCEE) (pp. 381-385). IEEE.
46. Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. Available at SSRN 2709713.
47. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151
48. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.
49. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society, 39, 283-297.
50. Ghosh, B. C., Ramakrishna, V., Govindarajan, C., Behl, D., Karunamoorthy, D., Abebe, E., & Chakraborty, S. (2021, May). Decentralized cross-network identity management for blockchain interoperation. In 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1-9). IEEE
51. Pongnumkul, S., Siripanpornchana, C., & Thajchayapong, S. (2017, July). Performance analysis of private blockchain platforms in varying workloads. In 2017 26th international conference on computer communication and networks (ICCCN) (pp. 1-6). IEEE

52. Vacca, A., Di Sorbo, A., Visaggio, C. A., & Canfora, G. (2021). A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges. Journal of Systems and Software, 174, 110891.
53. Musungate, B. N., Candan, B., Çabuk, U. C., & Dalkılıç, G. (2019, October). Sidechains: Highlights and challenges. In 2019 Innovations in Intelligent Systems and Applications Conference (ASYU) (pp. 1-5). IEEE
54. Yadav, A. S., Singh, N., & Kushwaha, D. S. (2022). Sidechain: storage land registry data using blockchain to improve the performance of search records. Cluster Computing, 25(2), 1475-1495
55. Montgomery, H., Borne-Pons, H., Hamilton, J., Bowman, M., Somogyvari, P., Fujimoto, S., ... & Belchior, R. (2020). Hyperledger cactus whitepaper. URL: https://github. com/hyperledger/cactus/blob/main/whitepaper/whitepaper. md.
56. Bradach, B., Nogueira, J., Llambías, G., González, L., & Ruggia, R. (2022, October). A gateway-based interoperability solution for permissioned blockchains. In 2022 XVLIII Latin American Computer Conference (CLEI) (pp. 1-10). IEEE.
57. Team, W. (2023). Weaver: Dlt interoperability framework. accessed Feb
58. Hyperledger Firefly: https://www.hyperledger.org/projects/firefly
59. Kang, I., Gupta, A., & Seneviratne, O. (2022, December). Blockchain Interoperability Landscape. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 3191-3200). IEEE.
60. Belchior, R., Vasconcelos, A., Correia, M., & Hardjono, T. (2022). Hermes: Fault-tolerant middleware for blockchain interoperability. Future Generation Computer Systems, 129, 236-251.
61. Yui, https://github.com/hyperledger-labs/yui-docs
62. Dinh, T. T. A., Datta, A., & Ooi, B. C. (2019). A blueprint for interoperable blockchains. arXiv preprint arXiv:1910.00985.
63. Bayraktar, S., & Gören, S. (2022, August). Design Principles for Interoperability of Private Blockchains. In The International Conference on Deep Learning, Big Data and Blockchain (pp. 15-26). Cham: Springer International Publishing.
64. Yang, L., Jiang, R., Pu, X., Wang, C., Yang, Y., Wang, M., ... & Tian, F. (2023). An access control model based on blockchain master-sidechain collaboration. Cluster Computing, 1-21
65. Hyperledger Cacti, https://www.hyperledger.org/projects/cacti
66. Hyperledger Besu, https://www.hyperledger.org/projects/besu
67. R3 Corda, https://r3.com/
68. Distributed metaverse: creating decentralized blockchain-based model for peer-to-peer sharing of virtual spaces for mixed reality applications B Ryskeldiev, Y Ochiai, M Cohen, J Herder - Proceedings of the 9th …, 2018 - dl.acm.org
69. Jiang, Hao, et al. “Channel modeling and characteristics for 6G wireless communications.” IEEE Network 35.1 (2020): 296-303.
70. Gadekallu, Thippa Reddy, et al. “Blockchain for edge of things: Applications, opportunities, and challenges.” IEEE Internet of Things Journal 9.2 (2021): 964-988.
71. Xie, Junfeng, et al. “A survey on the scalability of blockchain systems.” IEEE network 33.5 (2019): 166-173.
72. Alghamdi, Turki Ali, Rabiya Khalid, and Nadeem Javaid. “A Survey of Blockchain-based Systems: Scalability Issues and Solutions, Applications and Future Challenges.” IEEE Access (2024).
73. Balani, Nisha, Pallavi Chavan, and Mangesh Ghonghe. “Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks.” Multimedia Tools and Applications 81.25 (2022): 36699-36713.
74. Singh, Amritraj, et al. “Sidechain technologies in blockchain networks: An examination and state-of-the-art review.” Journal of Network and Computer Applications 149 (2020): 102471.
75. https://loomx.io/
76. Punathumkandi, Swathi, Venkatesan Meenakshi Sundaram, and Prabhavathy Panneer. “Interoperable permissioned-blockchain with sustainable performance.” Sustainability 13.20 (2021): 11132.
77. Sestrem Ochôa, Iago, et al. “A cost analysis of implementing a blockchain architecture in a smart grid scenario using sidechains.” Sensors 20.3 (2020): 843.

 doi:10.20944/preprints202501.2195.v1



78. Pathak, Aditya, Irfan Al-Anbagi, and Howard Hamilton. "SATI: Sidechain-Based Access Control & Trust Mechanism for IoT Networks." IEEE Transactions on Network and Service Management (2024)