Challenges and trends of Blockchain Interoperability and multi-blockchain architectures

Pedro M. R. G. Silva [1], **Matheus Lázaro Honório da Silva**[1], **Gislainy Velasco**[1], **Sergio T. Carvalho**[1]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)

mrgpedrosilva@gmail.com

sergiocarvalho@ufg.br

{matheus.lazaro, gislainycrisostomo }@discente.ufg.br

Abstract. *The blockchain landscape in healthcare has undergone significant transformations, transitioning from large public networks to customizable and private blockchains, raising questions about how to integrate multiple blockchains into a unified system. This paper examines emerging trends and persistent challenges in blockchain interoperability within healthcare data-sharing systems. We investigate solutions including Polkadot, Hyperledger Cacti, and Cosmos, revealing gaps: the absence of general protocols for heterogeneous blockchain communication, reliance on external trust rather than cryptographic consensus in multi-chain transactions, and inadequate identity verification mechanisms. We identify Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs) as promising approaches for the identity challenge, and multi-blockchain consensus protocols as an unexplored solution where nodes from multiple chains collaboratively validate cross-chain transactions.*

1. Introduction

Since its popularization through the Bitcoin network, blockchain and other distributed ledger technologies (DLTs) have been explored as solutions to enhance security, data integrity, transparency, and accountability across various domains. In the Internet of Things (IoT), several studies [Wang et al. 2022, Liu et al. 2020, Alghuried et al. 2025] propose architectures that leverage blockchain's intrinsic properties, such as data immutability, availability, and transparency, to address the inherent security vulnerabilities in IoT communication. This concept extends to smart cities [Liu et al. 2020], where blockchain and other DLTs enable the secure, transparent, and potentially anonymous storage of data from innovative vehicles.

Blockchain technology also holds significant potential in the healthcare sector. Researchers, such as [Wu et al. 2025, Gohar et al. 2022, Song et al. 2023], advocate for its use as a data-sharing mechanism that ensures transaction traceability and immutability. Additionally, some AI researchers explore blockchain's decentralized architecture to enhance machine learning training, leveraging the distributed nature of blockchain networks, which typically connect numerous peers. As Distributed Ledger Technologies (DLTs) evolve beyond crypto mining and exchange, interest in enabling communication and interoperability between blockchains has grown [Song et al. 2023, Belchior et al. 2023].

From this, the term ”multi-blockchain network” was then created to categorize architectures that comprise more than one independent blockchain system, as seen in [Malamas et al. 2023, Wu et al. 2025].

This paper aims to identify trends and challenges in blockchain interoperability and multi-blockchain architectures, with a specific focus on the healthcare sector. It's organized into a ”Related Works” section and a ”Fundamentals” section, in which we provide the basic knowledge on blockchain. In this section on multi-blockchain architectures, we discuss what cross-chain communication is and propose solutions for blockchain interoperability. We then proceed to a trends and challenges section, where the challenges identified and some recent research trends are discussed.

2. Related work

Researchers have increasingly explored methods to enable interoperability between DLTs in recent years. Notable reviews on this topic include [Belchior et al. 2023], which conducted an extensive investigation into blockchain interoperability capabilities and the techniques used to achieve it, such as Hash Lock Time Contracts (HTLCs), Relay/Sidechains, and Notary Schemes. The authors also worked on defining cases where blockchain interoperability models are needed. Similarly, [Haugum et al. 2022] provides an extensive review of blockchain interoperability definitions and the techniques primarily noted as means to enable it.

The work [Malamas et al. 2023] introduces the concept of a Hierarchical Multi-blockchain design for various domains. In this system, users interact only with a proxy blockchain, which redirects requests through an Inter-blockchain API. Similarly, [Wu et al. 2025] proposes a cross-chain communication system that models relay nodes to monitor multi-chain transactions and proxy nodes to execute smart contracts within the relay network, handling credential forwarding. The authors of [Hashim et al. 2024] envision a system that leverages global smart contracts to facilitate asset exchange between two blockchains.

As systems tend to evolve based on society's needs and demands, blockchain-based healthcare systems appear to be following a similar path. A plethora of initiatives have explored private blockchains as an enabler for their proposals. Considering the healthcare context, we can see works that, in different ways, see blockchain as a place to store relevant information [Suciu et al. 2022, Pandey et al. 2023, Ajayi et al. 2020, Chakraborty et al. 2019, Lee et al. 2020, Zhu and Chen 2021], and as described by [Malamas et al. 2023], healthcare, together with other complex and critical ecosystems such as civil aviation and the energy sector, are ecosystems where interoperability is one basic prerequisites when building a solution. Still, the multi-blockchain architecture is maturing and evolving significantly in terms of blockchain interoperability. Thus, this paper presents a holistic view of existing multi-blockchain research, aiming to inform future and current research by identifying trends and challenges in the topic.

3. Fundamentals

In this section, we'll cover the fundamentals of blockchain, consensus, and cross-chain communication.

3.1. Blockchain

Blockchain and other Distributed Ledger Technologies (DLT) are essentially distributed ledgers where the ledger content must be the same in every node, with these ledgers stored in a blockchain, a data structure consisting of linked blocks. Each block contains transactions that are ordered inside the tree. The link between the blocks is established by storing the hash of the previous block in the block header, along with the nonce and the Merkle tree root [Nakamoto 2009].

Blockchains can be classified considering two aspects: blockchain node participation and consensus participation. Considering node participation access, we can classify a blockchain network as either public or Private. Public blockchains, such as Bitcoin and Ethereum, are networks where anyone can join and operate a blockchain node. Private blockchains, such as Hyperledger Fabric, are those where, for a node to join the network and have access to the chain state, it must be authorized by the network management [Haugum et al. 2022, Zhang et al. 2019]. Considering the consensus participation, besides public networks, we can have private and consortium blockchains. On private blockchains, the nodes that participate in the consensus are governed by a single organization or authority. Consortium blockchains have nodes governed by multiple authorities; therefore, the consensus is performed by a consortium [Zhang et al. 2019].

3.2. Consensus

In decentralized systems, all nodes in the network must reflect the same state. Therefore, on blockchain networks, a consensus mechanism is implemented to regulate the changes to the blockchain state. In Bitcoin, the consensus mechanism is used to choose which node will attach a block to the blockchain.

1. **Proof of Work**: Introduced by Nakamoto [Nakamoto 2009], proof of work consists of a computational challenge where the first node that finds a solution earns the right to add a node into the blockchain [Lashkari and Musilek 2021, Nakamoto 2009, Song et al. 2023].
2. **Proof of Stake**: Proof of stake is an alternative to proof of work in which, to reduce the energetic costs, the nodes can bid an amount of coins to raise their chances of being chosen to add the following block into the blockchain [Lashkari and Musilek 2021, Nakamoto 2009, Song et al. 2023].
3. **Proof of Authority**: Proof of authority is used mainly in private blockchains, where the nodes that will perform the consensus and validation are defined by the network administrators, and act together to validate new blocks [Lashkari and Musilek 2021, Song et al. 2023].

4. Multi-blockchain architectures

Multi-blockchain architectures are defined as systems that contain two or more independent blockchains, and in recent years, they have been observed in various approaches. In this section, we'll present an overview of cross-chain communication and discuss how it's done on Relay models, Polkadot, Hyperledger Cacti, and Cosmos.

4.1. Cross-chain communication

Cross-blockchain communication, as defined in [Bellaj et al. 2022, Belchior et al. 2023], refers to a process that starts in one blockchain and ends in another. According to

[Alghuried et al. 2025], blockchain interoperability occurs in three modes: Data Transfer, Asset Transfer, and Asset Exchange. In Data Transfer, one blockchain copies data to another. In Asset Transfer, assets move from one blockchain to another, with the source blockchain either burning or locking the asset, making it exist only on the destination blockchain. In Asset Exchange, participants perform atomic asset transfers, requiring all participants to be present on both blockchains.

As detailed by [Belchior et al. 2021, Zamyatin et al. 2021], no cross-chain protocol can tolerate misbehaving nodes without a third-party entity, meaning a blockchain is not able to validate a transaction that happened on another blockchain because it can't simulate the other blockchain's consensus in an acceptable time. Therefore, for the mentioned cross-chain communication solutions to work, it's necessary to assume that the transaction data is valid, which occurs by assuming trust in the consensus algorithm. In other words, because a consensus protocol is needed for blockchain systems, these solutions assume that the consensus is correct and can tolerate misbehaving nodes.

4.2. Relay

Relays are one of the most mentioned techniques regarding cross-chain communication. It started as a division between one mainchain and many sidechains, where the mainchain would have an asset ledger, allowing it to understand changes on the sidechains [Haugum et al. 2022]. As time passes, the concept of relay has evolved into something more generic, where one blockchain can trigger transactions/contracts/chaincodes on another blockchain [Belchior et al. 2022, Wood 2018].

4.3. Polkadot

Polkadot is an initiative led by one of the Ethereum co-founders, Dr. Gavin Wood [Wood 2018, Eldin et al. 2022], and it aims to create an environment for blockchain interoperability. Often cited as a Layer 0 blockchain, Polkadot is a relay-based infrastructure where a single relay chain connects the parachains. For connecting the parachains, Polkadot utilizes bridges, a specialized type of blockchain that contains the necessary information and data for using the relay chain [Eldin et al. 2022, Wood 2018]. Polkadot categorizes itself as a heterogeneous environment, given that the parachains can be built in different ways and have their own governance and structure; however, Polkadot does not connect to chains outside of its infrastructure.

4.4. Hyperledger Cacti

Hyperledger Cacti is a Hyperledger project that aims to enable interoperability between Hyperledger blockchains, such as Besu and Fabric. It's described as a "pluggable interoperability framework" and is a fusion between Hyperledger Cactus and Weaver. It allows two ledgers to share data through two main flows: Relay or Node servers. Both of them perform actions through a connector. This blockchain-specific layer includes contracts and validators, and has the necessary permissions to execute chaincodes and smart contracts on their respective blockchains. Thus, for a blockchain to share data, one of them initiates the process by calling the relay/node server, which triggers the relay/node server on the destination blockchain to execute a contract and add the new data to the blockchain (Figure 1). [Belchior et al. 2022]

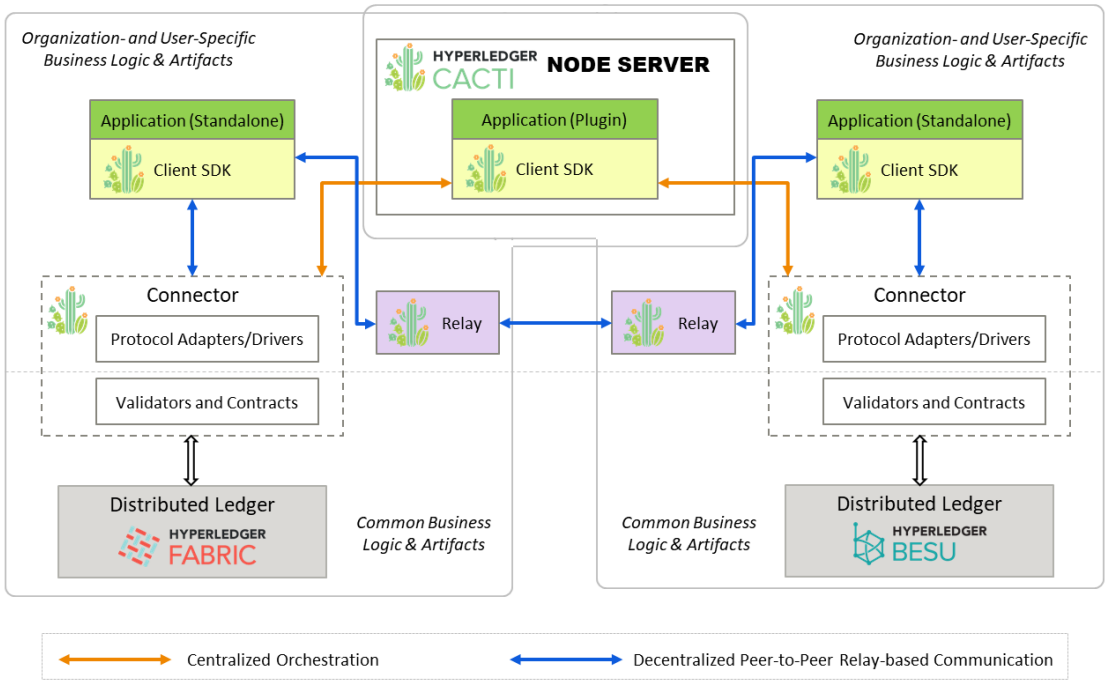

Figure 1. Hyperledger Cacti overview

4.5. Cosmos

Similar to Polkadot, Cosmos is an infrastructure based on relay chains that connect smaller chains. As an attempt to create ”the internet of blockchains”, it is divided into zones that are linked into hubs. The zones are composed of multiple independent chains running a Tendermint BFT consensus that are connected into a hub. Hubs, in turn, are blockchains that store information about assets exchanged between zones, in other words, a relay chain [Ethan Buchman 2016]. Cosmos relies on the Inter-Blockchain Communication (IBC) as a communication protocol between the hubs and the zones, which exchange tokens using IBC (Figure 2). Cosmos also created a protocol to enable transactions from zones into Ethereum and Bitcoin. [Eldin et al. 2022, Ethan Buchman 2016, Wood 2018].

5. Trends and Challenges

Blockchain-based systems have undergone significant changes in recent years, shifting from a single, massive public blockchain, such as Ethereum, to smaller and more customizable blockchains. In Healthcare systems, this can be easily perceived, as most recent studies on data sharing models rely on private blockchains, such as Hyperledger Fabric [Liu et al. 2020, Wu et al. 2025, Taherdoost 2023]. Now, we’re seeing attempts to make isolated blockchains capable of sharing data while preserving the intrinsic characteristics of blockchains [Belchior et al. 2022, Wu et al. 2025, Gohar et al. 2022, Song et al. 2023, Malamas et al. 2023, Belchior et al. 2023].

Regarding healthcare systems, there’s been a consistent focus on creating a governance system for Electronic Health Records (EHR), in which the blockchain can assume different roles [Lee et al. 2020, Chakraborty et al. 2019, Zhu and Chen 2021,

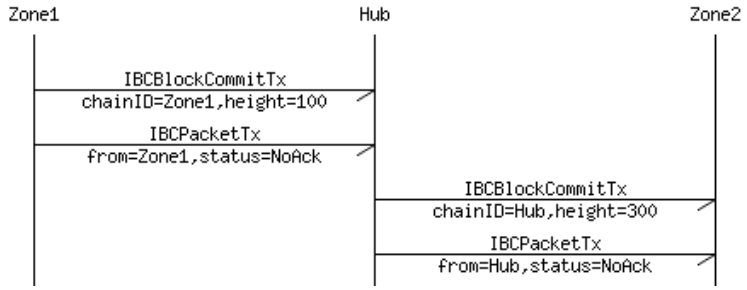

Figure 2. Cosmos Inter-Blockchain protocol

Ajayi et al. 2020, Pandey et al. 2023, Suciu et al. 2022]. Looking into the healthcare context and this focus on multi-blockchain architectures, we can identify some challenges:

- **Heterogeneous blockchain systems**: Currently, proposed solutions for homogeneous blockchain communication include Polkadot and stack-specific solutions such as Hyperledger Cacti; however, a general protocol for inter-blockchain communication is still under discussion [Belchior et al. 2023, Belchior et al. 2022]. Cosmos is an attempt to define a general Inter Blockchain Communication protocol, but its scope it's still limited and, when dealing with sensitive data, the fact that a Hub needs to store asset data in order to enable asset exchange is a problem. Cosmos is also not an academic consensus when projecting multi-blockchain architecture [Malamas et al. 2023, Liu et al. 2020, Pandey et al. 2023, Belchior et al. 2021]
- **Shared consensus**: The current solutions for blockchain interoperability share one common approach, the trust assumption on other systems. Therefore, there's a challenge in validating a transaction that occurs across multiple blockchains. One approach that has yet to be discussed is the possibility of a multi-blockchain consensus protocol, in which nodes from each blockchain participate in validating transactions. Having its own nodes participating in the consensus algorithm would lessen the external trust assumptions.
- **Sensitive data sharing**: As mentioned above, blockchain usage in data sharing systems is a powerful tool due to its immutability of transaction data and accountability. There's a search for enabling governance on sensitive data in a way that allows the data owner to control who has access to their data and can easily audit this information [Lee et al. 2020, Zhu and Chen 2021]. However, blockchain has some intrinsic features, for example the way in which data is saved and used inside the ledgers, that represents challenges when dealing with sensitive data protection regulations such as LGPD (Brazil) and GDPR(Europe). Thus, some researches have been using zero knowledge proof algorithms (ZPK) to modify the data access inside the blockchain and perform consensus in a way that it comply to data protection regulations [da Silva et al. 2025].
- **Identity verification**: Another challenge in blockchain systems on healthcare is how to identify a person inside the blockchain. Currently, the signatures on blockchain systems are done using asymmetric keys, which do not allow for deriving an identity from a key. Recent studies have focused on utilizing decentralized identifiers (DIDs) and self-sovereign identity (SSI) models to validate identities within the blockchain [da Silva et al. 2025, Bai et al. 2022, Xu et al. 2019].

6. Conclusion

In this paper, we present an overview of blockchain interoperability models and techniques, with a focus on the healthcare context. It was possible to identify several discussion topics, including heterogeneous blockchain systems, sensitive data sharing mechanisms, and Identity verification on blockchain systems. We also look into shared consensus model as a potential and unexplored solution for achieving consensus on multi-blockchain transactions, which will be explored in future research.

References

Ajayi, O., Abouali, M., and Saadawi, T. (2020). Secured inter-healthcare patient health records exchange architecture. In *2020 IEEE International Conference on Blockchain (Blockchain)*, pages 456–461.

Alghuried, A., Alkinoon, M., Mohaisen, M., Wang, A., Zou, C. C., and Mohaisen, D. (2025). Blockchain security and privacy: Threats, challenges, applications, and tools. *Distrib. Ledger Technol.* Just Accepted.

Bai, T., Hu, Y., He, J., Fan, H., and An, Z. (2022). Health-zkidm: A healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, 22(20).

Belchior, R., Borne-Pons, H., Hamilton, J., Bowman, M., Somogyvari, P., Montgomery, H., Fujimoto, S., Takeuchi, T., and Kuhrt, T. (2022). Cacti/whitepaper/whitepaper.md at 7bb39576080592919bea0ac89646b32105e1748e · hyperledger-cacti/cacti.

Belchior, R., Riley, L., Hardjono, T., Vasconcelos, A., and Correia, M. (2023). Do you need a distributed ledger technology interoperability solution? *Distrib. Ledger Technol.*, 2(1).

Belchior, R., Vasconcelos, A., Guerreiro, S., and Correia, M. (2021). A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput. Surv.*, 54(8).

Bellaj, B., Ouaddah, A., Bertin, E., Crespi, N., and Mezrioui, A. (2022). Sok: A comprehensive survey on distributed ledger technologies. In *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–16.

Chakraborty, S., Aich, S., and Kim, H.-C. (2019). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pages 260–264.

da Silva, M. H., Velasco, G., Vaz, N. P., Martins, M., Silva, P. R. G., and Carvalho, S. (2025). Blockchain and self-sovereign identity: A healthcare use case. In *Anais do VIII Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, pages 154–167, Porto Alegre, RS, Brasil. SBC.

Eldin, A. M., Hossny, E., Wassif, K., and Omara, F. A. (2022). Survey of blockchain methodologies in the healthcare industry. In *2022 5th International Conference on Computing and Informatics (ICCI)*, pages 209–215.

Ethan Buchman, J. K. (2016). Cosmos. Technical report.

Gohar, A. N., Abdelmawgoud, S. A., and Farhan, M. S. (2022). A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and iot. *IEEE Access*, 10:92137–92157.

Hashim, F., Shuaib, K., Baraka, E., and Sallabi, F. (2024). Enhancing ehr sharing through interconnected blockchains via global smart contracts. *International Journal of Computing and Digital Systems*, 16(1):1579 – 1591. Cited by: 1; All Open Access, Gold Open Access.

Haugum, T., Hoff, B., Alsadi, M., and Li, J. (2022). Security and privacy challenges in blockchain interoperability - a multivocal literature review. In *Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering*, EASE '22, page 347–356, New York, NY, USA. Association for Computing Machinery.

Lashkari, B. and Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, 9:43620–43652.

Lee, A. R., Kim, M. G., Won, K. J., Kim, I. K., and Lee, E. (2020). Coded dynamic consent framework using blockchain for healthcare information exchange. In *2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, pages 1047–1050.

Liu, J., Zhang, G., Sun, R., Du, X., and Guizani, M. (2020). A blockchain-based conditional privacy-preserving traffic data sharing in cloud. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pages 1–6.

Malamas, V., Palaiologos, G., Kotzanikolaou, P., Burmester, M., and Glynos, D. (2023). Janus: Hierarchical multi-blockchain-based access control (hmbac) for multi-authority and multi-domain environments. *Applied Sciences (Switzerland)*, 13(1). Cited by: 5; All Open Access, Gold Open Access, Green Open Access.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Technical report.

Pandey, S., De, A. K., Choudhary, S., and Asim, M. (2023). A decentralized blockchain-based architecture for healthcare industry. In *2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, volume 1, pages 1–5.

Song, R., Xiao, B., Song, Y., Guo, S., and Yang, Y. (2023). A survey of blockchain-based schemes for data sharing and exchange. *IEEE Transactions on Big Data*, 9(6):1477–1495.

Suciu, G., Balanescu, M., Mitroi, S., Trufin, D., Falahi, M., Şerban, C., and Goga, N. (2022). An overview of blockchain technology in stamina project. In *2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health)*, pages 1–4.

Taherdoost, H. (2023). The role of blockchain in medical data sharing. *Cryptography*, 7(3).

Wang, T., Wang, Q., Shen, Z., Jia, Z., and Shao, Z. (2022). Understanding characteristics and system implications of dag-based blockchain in iot environments. *IEEE Internet of Things Journal*, 9(16):14478–14489.

Wood, G. (2018). Polkadot: Vision for a heterogeneous multi-chain framework. Technical report, Polkadot.

Wu, Z., Wang, Y., and Wang, L. (2025). Gam: A scalable and efficient multi-chain data sharing scheme. *Information Processing and Management*, 62(3). Cited by: 0.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., and Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things Journal*, 6(5):8770–8781.

Zamyatin, A., Al-Bassam, M., Zindros, D., Kokoris-Kogias, E., Moreno-Sanchez, P., Kiayias, A., and Knottenbelt, W. J. (2021). Sok: Communication across distributed ledgers. In Borisov, N. and Diaz, C., editors, *Financial Cryptography and Data Security*, pages 3–36, Berlin, Heidelberg. Springer Berlin Heidelberg.

Zhang, R., Xue, R., and Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys*, 52:51.

Zhu, T.-L. and Chen, T.-H. (2021). A patient-centric key management protocol for healthcare information system based on blockchain. In *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–5.