Chapter 3
Blockchain Interoperability from the Perspective of Interdependent Networks

In this chapter, we discuss blockchain interoperability from the perspective of interdependent networks. At first, we define blockchain interoperability and present a high-level architecture view. After that, we discuss the design philosophy of blockchain interoperability that includes different interoperable blockchain considerations. Furthermore, we show a comparison of existing blockchain schemes. To the end, we present open issues with challenges and highlight some research directions on the blockchain interoperability domain (Fig. 3.1).

3.1 Interoperability Definition

Next generation blockchain systems will be powered by large and distinct blockchain networks. Such systems would need to enable cross-chain mechanisms to improve capabilities and upgrade functionalities in the future landscape. *Blockchain Interoperability* holds the same theme by enabling multiple blockchains to work together. A classic blockchain $\mathcal{B}_1$ allows a transaction when it maintains the $\mathcal{B}_1$'s rules considering the present state of $\mathcal{B}_1$. In the same way, a blockchain $\mathcal{B}_1$ is interoperable with another chain $\mathcal{B}_2$ and accepts transactions if that transaction does not transgress the rules.

Definition (Blockchain Interoperability) Let $\mathcal{B}_1 = \big(\mathcal{L}_{\mathcal{B}_1}, \mathcal{S}_{\mathcal{B}_1}$, Emission$_{\mathcal{B}_1}$, Mining$_{\mathcal{B}_1}$, Consensus$_{\mathcal{B}_1}$) and $\mathcal{B}_2 = \big(\mathcal{L}_{\mathcal{B}_2}, \mathcal{S}_{\mathcal{B}_2}$, Emission$_{\mathcal{B}_2}$, Mining$_{\mathcal{B}_2}$, Consensus$_{\mathcal{B}_2}$) be two blockchains. Let δ_{B_1} and δ_{B_2} be two sets that contain all possible values for the ledgers of $\mathcal{L}_{B_1}$ and $\mathcal{L}_{B_2}$, respectively. Now, blockchain $\mathcal{B}_1$ is regarded as interoperable with blockchain $\mathcal{B}_2$ if there exist

- a transaction $t \in \mathcal{T}$,
- a non-empty subset $\omega_{\mathcal{B}} \subset \delta_{\mathcal{B}_1}$, and $\omega_B \subsetneq \delta_{B_2}$ and

A. Imteaj et al., *Foundations of Blockchain*, SpringerBriefs in Computer Science,
https://doi.org/10.1007/978-3-030-75025-1_3

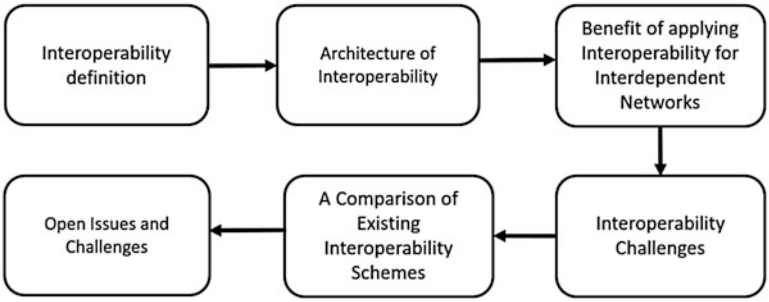
Interoperability definition
Architecture of Interoperability
Benefit of applying Interoperability for Interdependent Networks
Interoperability Challenges
A Comparison of Existing Interoperability Schemes
Open Issues and Challenges

Fig. 3.1 Chapter overview

- there exists such a block that contains transaction t, which is accepted by Consensus_{B_1} if $\mathcal{L}_{\mathcal{B}_1} \times \mathcal{L}_{\mathcal{B}_2} \in \omega_{\mathcal{B}_1} \times \omega_{\mathcal{B}_2}$, and otherwise, rejected.

3.2 An Architecture of Interoperability

The architecture of interoperability needs to be constructed in such a way so that security, traceability, and irreversibility are ensured in all the participated chains. For convenience, we can consider two chains (e.g., a blockchain for an energy network and another one for a transportation network) that wish to share data and exchange information. The chain that shares data is called source chain, and the receiver is called the destination chain. Suppose we enable interoperability by reading from the source chain and writing on the destination chain further. In that case, there may be a security concern for such an indirect interaction as the notary may tamper the shared data. As a result, the effectiveness of the interoperability can be degraded. To resolve the issue, a direct interaction paradigm can be effective for interoperability, which is presented in Fig. 3.2. In such a paradigm, data can be retrieved and transferred between two blockchains (that may reside in different blockchain networks, e.g., transportation, energy, water, or financial networks [1]) without any notary for maintaining effective performance and security of the blockchain ecosystem. Therefore, interoperability can be regarded as an intelligent characteristic that allows direct information exchange from one chain to another while preserves the essence of the participated blockchains. The cross-chain framework generally consists of five layers that work together to handle the issues related to interoperability, which are discussed below.

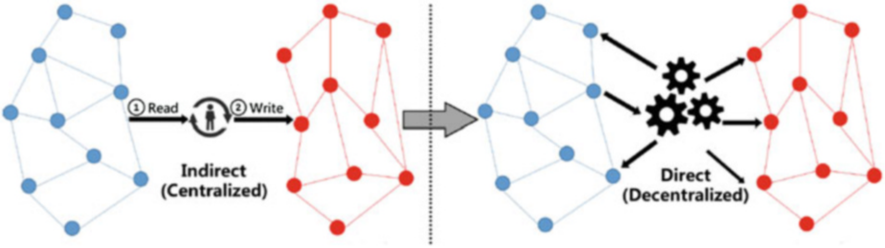

Fig. 3.2 A high-level architecture of blockchain interoperability [2]

3.2.1 Data Generation in Data Layer

One of the most important tasks in blockchain systems is to manage data that includes maintaining block structure, transaction format, modeling storage, etc. Blockchain systems may vary in terms of the data layers, and diverse transaction format is one of the bottlenecks for enabling information exchange across multiple blockchains. For instance, the data format of Bitcoin and Ethereum is not similar that results in impediments while making a transaction between Bitcoin and Ethereum. One possible solution is to create a unified transaction format that is facilitated by the data generator module. A middleware can be built with a data generator that allows direct interaction among multiple blockchains. The blockchain ecosystems can easily adapt the unified transaction format and make a connection with the middleware. However, there would add more complexity if we change each existing blockchain's transaction format, rather than a transaction translator can help translate the transactions from a blockchain's specific format to a unified one.

3.2.2 Cross-Chain Mechanism in Network Layer

The main purpose of the network layer in the blockchain is to maintain communication among available nodes. To leverage the decentralization nature and carry out intra-blockchain communication, P2P protocol, gossip protocol, or a combination of P2P and gossip protocols is widely used. Besides, a cross-chain communication mechanism is proposed by [2] to enable inter-blockchain communication for ensuring interoperability. However, the cross-chain communication may arise several issues, i.e., discovering IP address of the counter blockchain without presence of any trusted authority or centralized server, obtaining notable performance, handling of consensus mechanism of the communicated blockchains.

3.2.3 Verification of Transaction in Consensus Layer

Another essential stage of blockchain interoperability is to verify the transaction in order to ensure the consistency of blockchain states. The consensus algorithms can be classified into two categories: Nakamoto consensus, which includes proof of work (PoW), proof of stake (PoS), proof of elapsed time (PoET), proof of location (PoL), etc. and classical consensus such as practical Byzantine fault tolerance (PBFT). During cross-chain communication, the consensus algorithms examine whether valid data is committed and shared from the source chain. Besides, the consensus algorithms can verify whether data has been tampered or not on the destination chain.

3.2.4 Smart Contract for Cross-Chain Mechanism in Contract Layer

To enable cross-chain communication between multiple blockchains, there needs to be constructed a smart contract that would hold all the transaction rules, policies, and agreements. That smart contract needs to be prepared on the consent of the participated nodes from the communicated blockchains. The smart contract would be triggered during a transaction between source and destination blockchains. However, the main challenge is to consider a unified programming language and runtime environments for source and destination blockchains since different blockchains may be constructed with different programming languages and runtime environments.

3.2.5 Application Programming Interface (API) in Application Layer

Finally, the interface for performing interoperability among multiple blockchains should be user-friendly. Many developers get interested in taking part in the developing process, and users can easily carry out the interoperable actions with other blockchain networks.

3.3 How Blockchain Interoperability Concept Can Be Useful for Interdependent Networks?

In a conventional system, networks are studied in an individualistic manner. With the ever-improvements of related technologies, the coupling of different networks has become a feasible task. Interdependent networks mean the dependency of different networks to execute their regular operations. For instance, transportation networks may need to know about the demand response status of a particular city that could be provided by energy networks. Similarly, water has direct relation with energy networks, or a financial network may perform necessary operations after exchanging information with energy networks. Now, suppose we apply blockchain for such interdependent networks. In that case, we need to apply blockchain interoperability that allows us to exchange data among multiple blockchains that may be different in architecture, protocols, consensus mechanism, and so on. Without enabling blockchain interoperability, data would be restricted only in a single chain; thus, the main theme of interdependent networks (i.e., sharing data) would not be achieved. However, enabling blockchain interoperability is not a straightforward task. Several technical challenges would arise while applying blockchain interoperability for interdependent networks, and we discuss those challenges in our next section.

3.4 Interoperability Challenges

The goal of establishing interoperability is not an easy task. Several challenges arise while applying interoperability across multiple chains: assurance of atomicity, security maintenance, improvement of efficiency, tolerance of diversification, and user-friendliness. However, there is no universal framework that can solve all the stated issues.

3.4.1 Assurance of Atomicity

The guarantee of atomicity for blockchain interoperability event is a challenging task. For interoperability, atomicity means any event that performs on the chains needs to be either completely successful or unsuccessful at the same time for both chains. For instance, we can consider two different financial companies (namely, A and B) that possess different blockchains and they try to transfer assets. A customer from company "A" named "X" wants to send some assets to a customer named "Y" from company "B." Now, if customer "X" transfers money to customer "Y," then customer "X"'s assets on chain "A" should decrease, while customer "y"'s asset on chain "B" should increase. Both of these events should be either successful or unsuccessful for a particular event.

3.4.2 Improvement of Efficiency

Blockchain interoperability is always challenging to maintain a stable cross-chain communication and accelerate the data exchange process. The interoperability process's performance affects multiple parties; hence, it deserves more attention to ensure a swift cross-chain operation. The efficiency can be accessed and determined by examining the chain interaction times in every second. The consensus mechanism that includes transaction validation, data commitment speed at the destination chain, effective cross-chain communication, smart contract, and verification module are regarded as the essential factors for improving blockchain interoperability.

3.4.3 Maintenance of Security

The cross-chain mechanism raises the security risks that could subvert the blockchain ecosystem's security. The cross-chain mechanism introduces more security risks than individual blockchain operations. The data transmission process of the cross-chain process has three phases: (1) the shared data is leaving the source chain, (2) the shared data leaves source chain and currently in transit, and (3) the shared data is reaching at the destination chain. These phases result in the necessity of undertaking different measures to consider for each phase. In particular, the security maintenance across multiple chains needs to satisfy the following: (a) the shared data collects from a random node, needs to commit on the source chain, and should be reliable, (b) the shared data while in transit cannot be tampered, and a signature checking mechanism can be incorporated, and (c) a final commitment should be encountered on the destination chain after the shared data reaches to the destination chain without any temperament.

3.4.4 Handling of Diversification

During blockchain interoperability, we may face diversification in terms of a consensus protocol or usage scenarios. The consensus mechanism of a company "M"'s blockchain may be distinct from the consensus of another company "N"'s blockchain due to their diverse business policies. Besides, several open-source blockchain source codes are available that could be customized by making some code changes, and it brings diversity in the usage scenarios within blockchain systems. That means very few changes are required when a new blockchain joins the blockchain ecosystems and the blockchains try to exchange information.

3.5 A Comparison of Existing Interoperability Schemes

A few interoperability schemes are available that vary in terms of interoperability, atomicity, universality, efficiency, and security. In Table 3.1, we present the comparison of some of the existing blockchain interoperability schemes.

3.6 Open Issues and Challenges

This section discusses the open issues and challenges related to blockchain interoperability, i.e., the adaptation of communication and data exchange mechanisms among multiple blockchains. It is challenging to ensure correct executions on a different blockchain without the presence of any trusted authority. Although notable recent advancement is made, there is still a marginal gap between theory and practical aspects in the blockchain interoperability domain.

It is not easy to coordinate different blockchain transactions to support cross-chain communication, as blockchains may vary in terms of architecture, access controls, protocols, and service discovery. Besides, it is complicated to revert a transaction that depends on another, particularly when transaction decisions are made in different blockchains. Although some solutions (e.g., [6]) toward this issue are proposed, they are still not rigorous to be applied in a complex cross-chain decentralized application (dApp). More extensive research is necessary to handle the issue effectively.

Some prior works (e.g., [7]) discussed problems regarding security, confidentiality, trust, and data privacy issues. These issues are exacerbated during the collaboration of multiple blockchains with their respective properties. Regarding privacy, if a user asks for the deletion of their shared personal data, there are no effective mechanisms to respond to that request. To minimize the leakage and confidentiality, blockchain fine-grained access control [8, 9] can be adapted. Furthermore, blockchain interoperability raises the risk of attacks [10, 11] due to variant access control, consensus algorithms, protocols, or service discovery in underlying cross-chain communication. In a nutshell, the most prominent open issues and challenges in blockchain interoperability areas are security and privacy [12–14], discoverability [15], and governance [16, 17].

Table 3.1 Comparison of existing blockchain interoperability schemes

Approach	Atomicity	Interoperability	Universality	Efficiency	Security
Notary [3]	Good	Medium	Poor	Good	Poor
Sidechains [4]	Good	Medium	Poor	Poor	Good
Hash-locking [5]	Good	Medium	Poor	Poor	Good
MMR [2]	Good	Good	Medium	Good	Good

3.7 Research Directions

For smooth operations of blockchain interoperability, new frameworks, protocols, and programming models are in the emerging process and still need further development. While protocols (e.g., UIP, ILP) enable cross-chain transactions, Cosmos [18] and Polkadot [19] programming models allow developers to create blockchain and make communication with other blockchain networks. However, if the communicated blockchain types (i.e., private, public, permissioned) are different, we may face trouble performing cross-chain communication. A few solutions are proposed in this regard, e.g., multichain [20] can connect to Bitcoin but has limited functionalities. Therefore, bidirectionally connecting various types of blockchains is an open research problem. In the light of prior research and identification of open research issues and challenges, we point out research directions on blockchain interoperability domain considering blockchain architecture, cryptocurrency, blockchain engines and connectors, tools, standards, programming languages, and others.

Blockchain Interoperability Design

- Designing an effective blockchain interoperability model by considering various levels of interoperability layers, e.g., technical layers that consider technical factors to integrate blockchains, and semantic layers that are concerned with preserving application-specific semantics across blockchains.
- Modeling different views based on interoperability types and stakeholders, e.g., technical view for provider on a dApp vs. semantic view for end user on the same dApp.

Managing Cryptocurrency for Blockchain Interoperability

- Developing protocols for allowing authorized money exchange.
- Improving level of security and privacy during decentralized cryptocurrency exchange.
- Developing solutions with the aim of obtaining optimal benefit from side chains for permissioned blockchains.

Blockchain Engines

- Developing blockchain engines to bridge permissioned blockchains with permissionless blockchain to evaluate effective interoperability for various blockchain types.

Blockchain Connectors

- Study how the trust of trusted parties that route transactions from source to a destination blockchain can be made decentralized and integrate with a public blockchain, i.e., periodically acknowledging the state to a public blockchain.
- Guarantee atomicity on cross-blockchain dApps.
- Improving consistency and integrity during cross-blockchain communication.

- Constructing blockchain migration schemes for permissioned and public ledgers by considering various functionalities set by stakeholders.
- Coupling newly developed blockchain engines with existing blockchain systems.

Supporting Tools, Standards, and Programming Languages

- Developing new tools, standards, programming languages, frameworks, and verifiable credentials for cross-blockchain mechanisms.
- An extensive study on security loopholes of blockchain interoperability.
- Examining the effectiveness of integrating cryptocurrency schemes, blockchain engines, and connectors for cross-chain decentralized applications.

3.8 Discussion

This chapter presents the blockchain interoperability concepts by presenting details about the cross-chain architecture and its layers. We discuss the importance of applying interoperability in interdependent networks and possible challenges in deploying cross-chain communication among multiple blockchains. Furthermore, we provide a comparison of existing blockchain schemes. To the end, we highlight the open issues and challenges considering the prior works and point out the research directions in blockchain interoperability domains from the perspective of interdependent networks.

References

1. Amini, M.H., Imteaj, A., Pardalos, P.M.: Interdependent networks: A data science perspective. Patterns **1**(1), 100003 (2020)
2. Jin, H., Dai, X., Xiao, J.: Towards a novel architecture for enabling interoperability amongst multiple blockchains. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1203–1211. IEEE (2018)
3. Hegnauer, T.: Design and Development of a Blockchain Interoperability API. Ph.D. diss., Master's thesis, CSG@ IFI, University of Zurich, Switzerland, to appear 2019. Supervisors: Eder Scheid, Bruno Rodrigues, Burkhard Stiller, 2019
4. Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., Wuille, P.: Enabling blockchain innovations with pegged sidechains, vol. 72 (2014). https://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains
5. Deng, L., Chen, H., Zeng, J., Zhang, L.-J.: Research on cross-chain technology based on sidechain and hash-locking. In: International Conference on Edge Computing, pp. 144–151. Springer, Cham (2018)
6. Besançon, L., Da Silva, C.F., Ghodous, P.: Towards blockchain interoperability: Improving video games data exchange. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 81–85. IEEE (2019)
7. Hoang Tam, V., Wang, Z., Karunamoorthy, D., Wagner, J., Abebe, E., Mohania, M.: Internet of blockchains: techniques and challenges ahead. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)

and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1574–1581. IEEE (2018)
8. Wang, S., Zhang, Y., Zhang, Y.: A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access **6**, 38437–38450 (2018)
9. Lin, C., He, D., Huang, X., Raymond Choo, K.-K., Vasilakos, A.V.: BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. J. Network Comput. Appl. **116**, 42–52 (2018)
10. Sai, K., Tipper, D.: Disincentivizing double spend attacks across interoperable blockchains. In: 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 36–45. IEEE (2019)
11. Borkowski, M., Sigwart, M., Frauenthaler, P., Hukkinen, T., Schulte, S.: DeXTT: Deterministic cross-blockchain token transfers. IEEE Access **7**, 111030–111042 (2019)
12. Casino, F., Dasaklis, T.K., Patsakis, C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics Informatics **36**, 55–81 (2019)
13. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
14. Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J.A., Liu, R.P.: Survey: Sharding in blockchains. IEEE Access **8**, 14155–14181 (2020)
15. Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., Hu, Y.-C.: Hyperservice: Interoperability and programmability across heterogeneous blockchains. In: ACM SIGSAC Conference on Computer and Communications (2019)
16. Hardjono, T., Lipton, A., Pentland, A.: Towards a public key management framework for virtual assets and virtual asset service providers. http://arxiv.org/abs/1909.08607
17. Hardjono, T., Lipton, A., Pentland, A.: Toward an interoperability architecture for blockchain autonomous systems. IEEE Trans. Eng. Manag. **67**(4), 1298–1309 (2019)
18. Cosmos Network: https://cosmos.network, Accessed 2019
19. Wood, G.: Polkadot: Vision for a heterogeneous multi-chain framework. White Paper (2016)
20. Greenspan, G.: MultiChain White Paper (2015). https://www.multichain.com/white-paper/