Enhancing Blockchain Interoperability through Sidechain Integration and Valid-Time-Key Data Access Control

Tuan-Dung Tran[1] [0000-0003-1156-7072], Kiet Anh Vo[2] [0009-0004-0883-1236], Nguyen Binh Thuc Tram[2] [0009-0006-0808-0019], Ngan Nguyen Bui Kim[2] [0009-0000-4936-468X], Phan The Duy[1] [0000-0002-5945-3712], and Van-Hau Pham[1] [0000-0003-3147-3356]

[1] Information Security Laboratory, University of Information Technology, VNU-HCM, Ho Chi Minh City, Vietnam
{dungtran,duypt,haupv}@uit.edu.vn

[2] Faculty of Computer Networks and Communications, University of Information Technology, VNU-HCM, Ho Chi Minh City, Vietnam
{20520605,20520815,20520648}@gm.uit.edu.vn

Abstract. Currently, the lack of interoperability poses a significant limitation for blockchain technology. Achieving cross-chain interoperability is crucial in enhancing the network's computing performance, storage capacity, and scalability. This research proposes a cross-chain architecture that allows interoperability and sharing capabilities to address the challenge and overcome the limitations of previous interchain interaction systems. The proposed system involves interchain data transfer using a Sidechain that incorporates a valid-time key (VTK) data access control scheme to facilitate blockchain data verification of multiple blockchain networks. In the context of healthcare data exchange, our experiments show that the proposed architecture effectively enables interchain communication and data transfer while ensuring the security and authenticity of the transferred information. The VTK mechanism successfully restricts access to authorized parties and ensures that the access is time-limited, thereby preventing unauthorized access and fraudulent activities.

Keywords: Access control · Blockchain interoperability · Cross-chain · Sidechain · Valid Time Key.

1 Introduction

Blockchain technology has gained extensive applications across a range of industries such as finance, insurance, healthcare, social support, and education [1]. However, research suggests that the issue of interoperability among diverse blockchains can give rise to challenges. Currently, in the realm of blockchain applications, collaboration among multiple entities within the same network is commonplace. However, for the technology to progress further, fostering interoperability between disparate chains is a crucial aspect [2]–[4]. In the healthcare sector, effective transparency is a cornerstone of success, enabling seamless interactions among parties. However, the fragmented storage of data in existing blockchain systems poses a challenge when it comes to sharing information among stakeholders, primarily due to discrepancies in storage and control system designs [5]. This fragmented and centralized information gives rise to notable information concerns, imposing significant limitations on the provision of data accuracy and high-quality patient care and treatment.

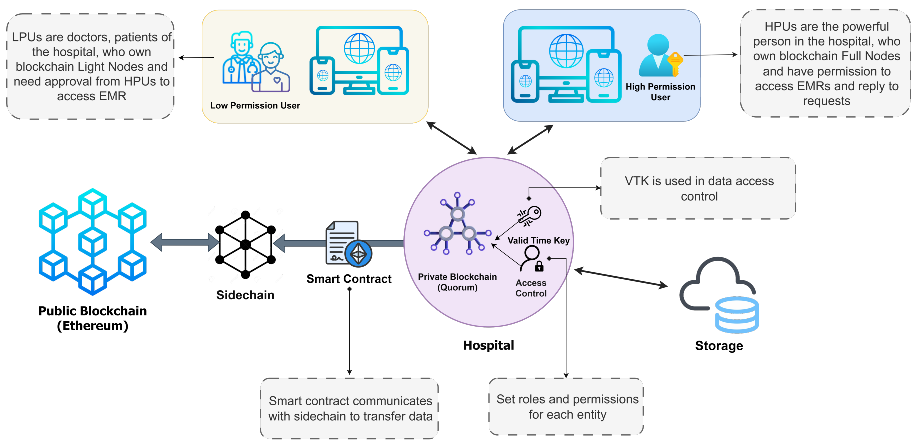

Fig. 1: The concept of cross-chain communication architecture in Healthcare

In the healthcare industry, centralized information management in healthcare faces considerable risks due to its high vulnerability to cyber attacks, resulting in the potential loss or theft of data [6], [7]. To facilitate the effective management and enhance patient care processes in healthcare facilities, the implementation of an interoperability mechanism is essential while ensuring robust security measures for the exchange of patient medical records [8]. Building and optimizing a cross-chain interaction support system for information verification is of utmost importance; nonetheless, current solutions present obstacles due to their high costs and intricate implementation processes.

To overcome the obstacle of transferring data between separate blockchains, our proposal introduces a sidechain of Oracle nodes. The sidechain serves as a communication bridge between two chains while ensuring data validity through verification by other nodes. Enforcing access control through VTK, our system ensures that data transfer and viewing are strictly limited to authorized parties only. With an unwavering focus on data security and privacy, our solution makes significant contributions in the following aspects:

– We propose a novel approach introducing an innovative interchain system that leverages the sidechain architecture to verify data transparency, incorporating access control through the implementation of the VTK mechanism.

- Our system was successfully implemented and tested on a network of blockchain platforms, resulting in fast and secure interchain mobility and data sharing. Performance, cost, and security were evaluated, with mostly positive results.

2 Related Works

In the pursuit of cross-chain interoperability and seamless execution of smart contracts across multiple networks, the adoption of standardized protocols and the application of innovative approaches emerge as pivotal factors. By embracing these remarkable advancements, the boundless potential of blockchain technology is unlocked, giving rise to an interconnected and collaborative ecosystem. [9], [10] and Buterin [11] have shed light on the importance of blockchain interoperability in their notable studies, with three primary categories of strategies: notary schemes, hash-locking, and relays/sidechain as essential frameworks for achieving seamless connectivity across diverse blockchain networks.

Notary Schemes: The notary scheme in the cross-chain approach offers a relatively simple solution. As elucidated by [12], this mechanism involves a trustworthy set of entities, acting as intermediaries, initiating actions in one blockchain in response to events taking place in another blockchain. Interledger[3] stands as a prominent and influential project in the realm of notary mechanisms. This protocol streamlines currency transfers between ledgers by leveraging a third-party connector, akin to the role of a notary in blockchain interoperability. However, reliance on a specific third party in notary technology can raise valid concerns regarding centralization, bottleneck, or blind trust.

Hash-locking: The utilization of hash locking as a cross-chain mechanism offers a streamlined approach to asset exchange removing the reliance on third-party involvement [13], [14]. In this process, both parties lock their exchangeable assets within the smart contract and send the hash value of a selected secret key to the recipient. The successful execution of the transaction relies on meeting the predetermined hash conditions within a specified timeframe. In the event that these requirements are not fulfilled, the assets are promptly returned to their rightful owners, ensuring a safeguarded process. While hash-locking serves as a viable solution for cross-chain asset exchange and transfer, it necessitates the compatibility of both involved chains to support the same hash function. This requirement can pose limitations in situations where the participating chains utilize distinct hashing algorithms or possess disparate technical prerequisites. Furthermore, a significant challenge lies in the high cost and intricate design requirements involved in ensuring mutual understanding and compatibility of smart contracts across different blockchains.

Relays/sidechain: is a promising cross-chain solution that places a premium on scalability and interoperability, offering a decentralized alternative compared to notary schemes. By leveraging this mechanism, the transfer of digital property, including assets, tokens, and data, becomes effortless and fluid

[3] https://interledger.org/

across disparate blockchain networks. Within the blockchain ecosystem, acting as an autonomous secondary blockchain, a sidechain operates independently, safeguarding the performance and security of the main blockchain without any adverse impact. Prominent blockchain interoperability platforms like Cosmos [15] and Polkadot [16] exemplify this concept by implementing an intermediary chain that fosters seamless and efficient cross-chain interactions.

The captivating realm of blockchain technology in the healthcare sector has drawn considerable interest from researchers, with a specific emphasis on its application in managing electronic medical records (EMRs) [17]. Unlocking the potential of blockchain technology, electronic medical records (EMRs) can find a safe sanctuary for storage, access, and sharing among authorized participants, preserving the utmost integrity and privacy of healthcare data. Nonetheless, when developing blockchain-based solutions, it is paramount to conduct a meticulous consideration of trade-offs, specifically with regard to security and interoperability.

3 Proposed System

Immersed in the environment of a hospital, the proposed system takes center stage as it empowers efficient management of patient health records through a robust and confidential blockchain network. However, the thing is the construction of such a network with multiple full nodes, responsible for preserving the complete blockchain history and verifying both transactions and new blocks, can often incur significant expenses that may be deemed prohibitive. Conversely, a network that predominantly features only a limited number of full nodes and numerous light nodes optimized for rapid transactions and daily activities can raise potential concerns regarding the integrity and confidentiality of stored electronic medical records (EMRs). In order to address this challenge, it becomes vital to establish verifiable evidence of data integrity, which can be securely stored on the public blockchain for the purpose of not only enhancing security but also enabling effortless retrieval of information when needed. Overcoming the obstacle of transferring data between blockchains with distinct architectures poses a significant challenge. To tackle this issue, our proposed solution, depicted in Figure 1, presents a comprehensive resolution, which will be elaborated upon in subsequent sections, providing an in-depth analysis of the system components in the subsequent sections. Table 1 presents a comprehensive list of the acronyms with a view to facilitating comprehension throughout the article.

3.1 Blockchain

To exemplify distinct blockchain architecture communication, our cross-chain model integrates Quorum [4]for the PriBC network and Ethereum for the PuBC network.

[4] https://consensys.net/quorum/

Table 1: Abbreviations and Acronyms

Abbreviation/Acronym	Definition
PuBC	Public blockchain
PriBC	Private blockchain
EMR	Electronic Medical Record
VTK	Valid Time Key
EID	EMR ID
UID	User ID
LPU	Low-Permission User
HPU	High-Permission User
LN	Light Node
FN	Full Node

1. Private Blockchain Network To fortify data security and streamline the process of data access requests, we implemented access controls using smart contracts on the Quorum blockchain. Within our private blockchain entities, three fundamental roles have been established:
   - Doctors, medical staff, and associated patients, being classified as LPUs, have the capability to request EMRs if granted access by full nodes.
   - Deans and managers, as prominent users within the system, hold pivotal roles and possess substantial permissions in validating EMRs, accessing content, and granting permissions to LPUs as needed.
   - Admins hold the utmost authority, taking on the pivotal responsibility of system management and addressing any emergent situations.
2. Public blockchain network
   Upon successful validation of an EMR by the FNs, the subsequent crucial step involves encryption of the EMR before it is securely stored in either cloud storage or the InterPlanetary File System (IPFS). Simultaneously, a unique hash value is generated through the process of hashing. The Ethereum blockchain acts as a secure repository for storing the hash value which is accompanied by the EMR's ID as a distinctive tag. The significance of these pieces of information cannot be denied, as they serve as compelling evidence during the validation process of the EMR. Moreover, upon requirement, the retrieval of the hash from Ethereum is seamless and hassle-free, further enhancing the overall efficiency and reliability of the system.

3.2 Sidechain

A sidechain is an innovative distributed network that empowers the validation and efficient transfer of data between two interconnected and diverse blockchains, commonly referred to as heterogeneous blockchains. The sidechain serves as a dynamic pathway, orchestrating the smooth transmission of hashes in reverse between the PriBC and PuBC networks, establishing a harmonious bridge for efficient communication and interoperability. Our proposed system incorporates a decentralized oracle network as the sidechain, facilitating the retrieval of external data into the blockchain and enabling the seamless transmission of internal blockchain data to the external realm. In the system, the oracle assumes a pivotal role with a multitude of responsibilities including receiving data requests from users, empowering the oracle contract to seamlessly transmit data outside the blockchain, and facilitating the provision of data to interconnected blockchains.

Within the sidechain realm, the indispensable role of each oracle comes to the fore as they fulfill user DApp requests and facilitate the seamless transfer of data between the interconnected blockchains. By leveraging smart contracts for interaction with the source blockchain, our system seamlessly facilitates on-demand data collection, including the retrieval of either newly generated hashes following the EMR hash or previously saved hashes linked to specific EMR IDs. When the data aligns with the new hash, a seamless transfer takes place, securely storing it on Ethereum, where it is uniquely identified by the EMR ID. Moreover, the successful execution of this operation hinges upon the presence of a crucial Ethereum smart contract, which assumes a pivotal role in the process. The comprehensive explanation of the process for querying the stored hash to perform integrity checks will be elaborated upon in section 3.4.

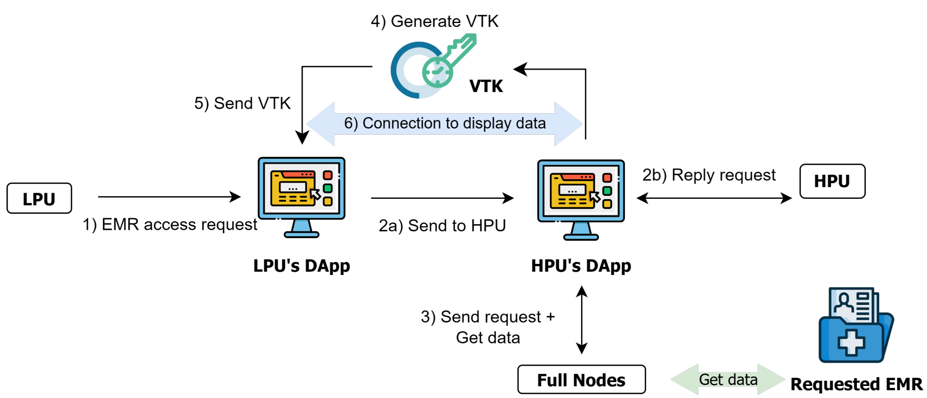

Fig. 2: The data-access request process.

3.3 Valid Time Key - VTK

In scenarios where LPUs seek access to encrypted data stored in the database, the utilization of a VTK becomes important in providing them with the required access privileges. During the process where a LN initiates a request to FNs, the content undergoes decryption by HPUs with a private key, contingent upon their approval. Following that, a connection is established, paving the way for the creation of a novel VTK, which is dispatched to the DApp of the LN that initiated the initial request. Armed with this valid time key, the DApp effortlessly establishes a secure connection, unveiling the gateway to access and comprehend the content of the data. Upon the expiration of the designated time, the validity of the time key ceases, triggering an instantaneous termination of the connection by the full nodes. As a consequence, the light nodes are effectively barred from accessing any information. Figure 2 showcases a detailed process model and Algorithm 1 offers a concise depiction of an EMR access control transaction using VTK.

Algorithm 1 EMR access control procedure

EMRAccessRequest $\leftarrow EID$ ▷ Step 1
if getApprovalFromHPU $\leftarrow UID$ **then** ▷ Step 2
  $decryptedEMR \leftarrow$ DecryptData($PrivateKey, EID$) ▷ Step 3
  $VTK \leftarrow$ Generation ▷ Step 4
  $dataConnection \leftarrow$ EstablishConnection $\leftarrow VTK, decryptedEMR$
  Send VTK to LPU ▷ Step 5
  while VTK is valid **do**
    $dataConnection \leftarrow VTK$ ▷ Step 6
  end while
  Close $dataConnection$
else
  NotifyClient("Don't get approval");
end if

3.4 Cross-chain data transfer

In this section, we delve into the elucidation of the transfer process for stored hash data from the public blockchain to the PriBC, which is vividly depicted in Figure 3. Electronic Medical Records (EMRs) undergo encryption and storage safeguarded by the secure custody of the private key lying in the hands of FNs. As a user initiates a request for hash verification of an EMR's integrity through the DApp, this meticulous process safeguards the utmost security of sensitive medical data and empowers authorized individuals to validate the authenticity of the EMR. Algorithm 2 offers a captivating insight into the sequential operations involved in the processing of EMR requests.

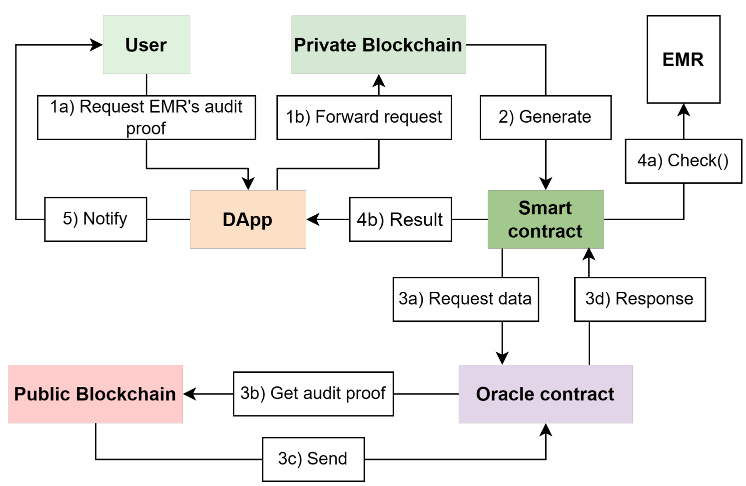

Fig. 3: The cross-chain data transfer process.

Step 1) EMR audit-proof, including hash and ID tag, is requested by clients from PuBC via DApp, which forwards the request to PriBC for processing. **Step 2)** The PriBC creates a smart contract and an oracle contract to communicate with the sidechain and retrieve data from the target blockchain. **Step 3)** The sidechain retrieves the requested data and transfers it to the PriBC. **Step 4)** The PriBC undertakes an integrity verification of the EMR by leveraging the hash value retrieved from the PuBC. **Step 5)** Ultimately, The DApp notifies the client of the results.

Algorithm 2 Verify the integrity of the EMR

Input: ID of the requested EMR
Output: Unmodified or Modified
Perform integrity verification of the EMR request ▷ Step 1
create Oracle contract ▷ Step 2
create PriBC smart contract
if isExistsInPuBC(ID) **then** ▷ Step 3
    $AuditProof \leftarrow$ Fetch
    Oracle node transfers $AuditProof$ to PriBC
else
    The transaction is canceled
    Exit
end if
$calHash \leftarrow hashCalculation \leftarrow EMR$ ▷ Step 4
$retrievedHash \leftarrow AuditProof$
if $calHash == retrievedHash$ **then**
    return Unmodified
else
    return Modified
end if
NotifyClient ▷ Step 5

4 Experiments and Results

4.1 Performance Evaluation

Throughout the experimental phase, we utilized three VMs, each equipped with a 4-core CPU, and a 60GB hard drive, 16GB of memory and operated on the Ubuntu 22.04 operating system. We evaluated the functionality of the system by conducting various activities such as registering an account on the DApp, sending access requests for EMRs through the DApp, granting timely access to requested EMRs using VTK, and revoking connection after the specified timeout. First, to estimate the performance, we record the duration of these transactions in Figure 4, and multiple measurements are made for each transaction to enhance accuracy and reliability. Based on the obtained experimental results, we evaluated the performance of transactions related to saving EMR to storage and data access control as highly satisfactory. As for the account registration activity on the DApp, it involves multiple steps, such as transaction creation on PriBC, identity verification, and authorization, which usually leads to slightly longer processing times compared to the transactions mentioned above. However, the overall results remain quite favorable. In the case of query transactions, which necessitate cross-chain interactions (described in Section 3.4), the measurement encompasses the time span from when the user submits the request until the receipt of the integrity check result. We assess that our proposed solution has demonstrated positive outcomes and holds potential for further advancement.

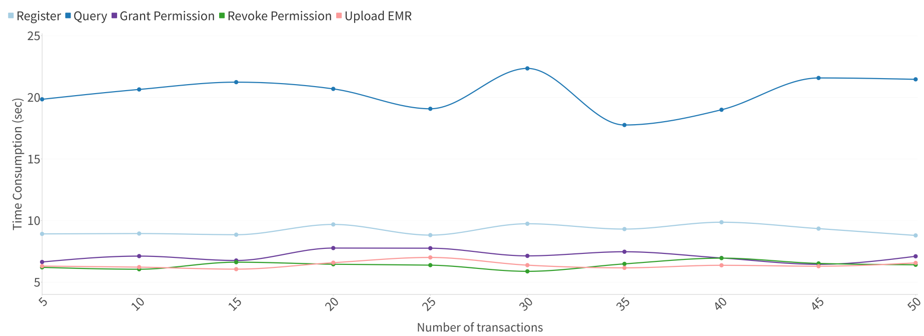

Fig. 4: Time consumption per transaction

We also perform the system's cost analysis based on the average value of multiple transactions. The transaction fee for each transaction is measured in gas unit, and the calculation results are shown in Table 2. The gas consumption for registering transactions for each entity in the blockchain is consistently equivalent, on average, and only needs to be performed once. The cost associated with storage, data access, and cross-chain transfer depends on the complexity of deployment and transmission. We assume that the incurred cost is reasonable and acceptable. Additionally, Table 2 provides insights into the CPU usage associated with each transaction. Among the examined processes, the query transaction engenders the highest CPU usage, accounting for an imposing 76.31%. Given the inherent limitations of our virtual machine's operation, the resulting CPU usage percentage may appear relatively substantial. However, this value remains well within acceptable limits and can be further enhanced through an upgrade of the hardware configuration. Currently, our smart contracts implementation is available online on GitHub[5].

4.2 Security Analysis

Our sidechain is a decentralized Oracle network that operates independently to ensure the proposed solution does not compromise the performance or security of blockchain networks. Each transaction is the responsibility of one Oracle node,

[5] https://github.com/Bingtoni2122/Sidechain-Integration-and-Valid-Time-Key

Table 2: The average cost consumption and CPU usage of transaction

Object	Transaction	CPU usage	Gas	USD
Blockchain Entities	Register Manager	66.29%	46407	4.46
	Register Doctor	66.17%	46378	4.45
	Register Patient	66.12%	46378	4.45
EMR	Store data	62.22%	92664	8.90
Data access control	Grant Permission	66.82%	161275	15.48
	Revoke Permission	66.60%	30261	2.91
Audit proof	Query	76.31%	229851	22.07

while the others verify the activity to ensure transparency and prevent fraudulent practices. Security of the transferred information and Restricts access: We ensure the security of transferred information by encrypting data throughout the transfer process, ensuring privacy and confidentiality even against man-in-the-middle attacks. Access control is achieved through a role-based division with varying permissions, limiting data verification requests to only the HPU to minimize the possibility of denial of service attacks. The deployment of VTK facilitates secure and convenient data access for clients while ensuring data privacy by granting permission only for a limited time. To prevent authenticity attacks, registering a new account requires consensus from other HPUs within the PriBC network, ensuring external attackers cannot gain unauthorized access or make fraudulent calls. Every account must be registered within the network, mapping verification, identity, and role information. When clients log in, our system checks all information and only accepts qualified accounts.

5 Conclusion

In this paper, we propose a blockchain interoperability solution using sidechain and Valid Time Key (VTK). Our sidechain is a decentralized network, serving as a trustworthy intermediary among heterogeneous blockchains. Additionally, we introduce the concept of a VTK to enhance secure data access management and convenience. Experimental results show that our system performs well in terms of functionality and cross-blockchain interaction. In future work, we aim to enhance system performance, optimize costs, and conduct further testing for external blockchain data. Moreover, we acknowledge the need to address mutable data scenarios and explore alternative methods for hash functions that can effectively verify the integrity of such data while compatible with blockchain technology.

References

[1] M. Rauchs, A. Blandin, K. Bear, and S. B. McKeon, "2nd global enterprise blockchain benchmarking study," *Available at SSRN 3461765*, 2019.

[2] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153 719–153 730, 2020.

[3] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, “Interoperability and synchronization management of blockchain-based decentralized e-health systems,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1363–1376, 2020.

[4] T. Hardjono, A. Lipton, and A. Pentland, “Toward an interoperability architecture for blockchain autonomous systems,” *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1298–1309, 2019.

[5] A. Roehrs, C. A. Da Costa, and R. da Rosa Righi, “Omniphr: A distributed architecture model to integrate personal health records,” *Journal of biomedical informatics*, vol. 71, pp. 70–81, 2017.

[6] N. Spence, M. Niharika Bhardwaj, and D. P. Paul III, “Ransomware in healthcare facilities: A harbinger of the future?” *Perspectives in Health Information Management*, pp. 1–22, 2018.

[7] N. Thamer and R. Alubady, “A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,” in *2021 1st BICITS*, IEEE, 2021, pp. 210–216.

[8] M.-H. Kuo *et al.*, “Opportunities and challenges of cloud computing to improve health care services,” *Journal of medical Internet research*, vol. 13, no. 3, e1867, 2011.

[9] S. Schulte, M. Sigwart, P. Frauenthaler, and M. Borkowski, “Towards blockchain interoperability,” in *Business Process Management: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, Proceedings 17*, Springer, 2019, pp. 3–10.

[10] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, “A survey on blockchain interoperability: Past, present, and future trends,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[11] V. Buterin, “R3 report-chain interoperability,” *R3 Res*, 2016.

[12] Z. Wang, J. Li, X.-B. Chen, and C. Li, “A secure cross-chain transaction model based on quantum multi-signature,” *Quantum Information Processing*, vol. 21, no. 8, p. 279, 2022.

[13] Monika, R. Bhatia, A. Jain, and B. Singh, “Hash time locked contract based asset exchange solution for probabilistic public blockchains,” *Cluster Computing*, vol. 25, no. 6, pp. 4189–4201, 2022.

[14] R. Bhatia, A. Jain, and B. Singh, “Hash time locked contract based asset exchange solution for probabilistic public blockchains,” *Cluster Computing*, vol. 25, no. 6, pp. 4189–4201, 2022.

[15] J. Kwon and E. Buchman, “Cosmos whitepaper,” *A Netw. Distrib. Ledgers*, p. 27, 2019.

[16] G. Wood, “Polkadot: Vision for a heterogeneous multi-chain framework,” *White paper*, vol. 21, no. 2327, p. 4662, 2016.

[17] M. V. Baysal, Ö. Özcan-Top, and A. Betin-Can, “Blockchain technology applications in the health domain: A multivocal literature review,” *The Journal of supercomputing*, vol. 79, no. 3, pp. 3112–3156, 2023.