MIDAS: A Multi-chain Interoperable Data and Access System for Healthcare

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

[1] Faculty of Computer Networks and Communications,
University of Information Technology,
Vietnam National University Ho Chi Minh City, Vietnam
{20520815,20520648}@gm.uit.edu.vn, dungtrt@uit.edu.vn

[2] Information Security Laboratory, University of Information Technology,
Vietnam National University Ho Chi Minh City, Vietnam
{duypt,haupv}@uit.edu.vn

Abstract. The emergence of Blockchain technology has inaugurated a transformative era by its multifaceted advantages and wide-ranging applications across diverse industries. Nevertheless, while holding great promise, Blockchain encounters a significant challenge in achieving interoperability within the complex landscape of multi-blockchain ecosystems. The imperative necessity for seamless data and digital asset exchange is evident, yet it is accompanied by the escalating complexities of managing network entity identities dispersed across disparate systems resulting in a stark dearth of cohesive connectivity and agile interaction. Henceforth, in response to these challenges, we present 'MIDAS' as a captivating research endeavor aimed at fostering seamless interoperability among a multitude of blockchain networks. MIDAS acts as a key intermediary, skillfully facilitating cross-chain interactions, elevating user experience, and ensuring secure data access for authorized users. In order to augmenting this architecture's prowess while also focusing on user-centric data control, we introduce a pioneering decentralized identity management system known as "Blockchain Interoperability Decentralized Identifier" (BIDI). BIDI offers a range of powerful features, including strict entity management, seamless connections, and customized data access controls for authorized users, with a focus on user-centric and data ownership. In other words, our framework is a significant step towards improving the effectiveness and versatility of blockchain technology, breaking down barriers for harmonious coexistence among multiple blockchains.

Keywords: Blockchain interoperability · Data access control · Decentralized identifiers · Sidechain · Healthcare

1 Introduction

Nowadays, blockchain has developed into a decentralized network system that can satisfy several crucial security requirements, including reliability, transparency and consensus of each transaction; as the capacity to guarantee data integrity and resilience against cyber attacks. However, as per [1, 2], 88% of blockchain applications involve several parties using the same blockchain network, 9% of them are cross-disciplinary, and 73% want to expand and strengthen their connections with new partners. As a result, the isolation of individual blockchains and the high degree of heterogeneity between them present a significant challenge for achieving interoperability, which is a major obstacle in the field of blockchain practical applications [3].

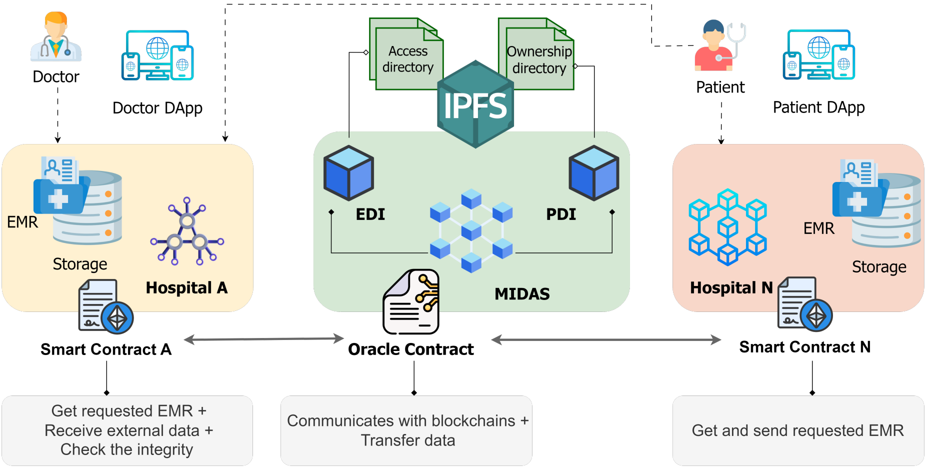

Fig. 1. The concept of MIDAS data transfer between multiple blockchains

In the pursuit of addressing the challenges of cross-chain interaction, our previous research introduced an innovative approach that leveraged a sidechain as an intermediary entity. The system was built as a decentralized oracle network, in which individual oracles undertook the pivotal role of facilitating seamless data transmission between the distinct blockchain systems involved. An oracle contract played a crucial role in ensuring smooth operation as it was enable robust communication with smart contracts across various blockchain networks. Despite advancements in prior systems, limitations persist in data access permissions and management within blockchain environments, especially in complex settings like hospital administration. A key challenge is the fragmentation of patient electronic medical records (EMRs) across diverse hospital blockchains, lead to hinder data linkage, management, and retrieving past EMRs faces obstacles from scattered data.

To address these limitations, this paper introduces a new architecture called Blockchain Interoperability Decentralized Identifier (BIDI). BIDI utilizes decentralized identifiers for blockchain entities to enhance data management and query efficiency across locations. It aims to improve data access permissions, eliminate administrative inefficiencies, and facilitate interoperability through streamlined data request, query, and transfer methods. The main contributions of our research are as follows:

- We propose a novel interchain system for transferring data named MIDAS.

- We implement the BIDI architecture to identify and manage entities in the system including people and data. We also integrate and store the BIDI on MIDAS for maximum efficiency for cross-chain interactive operations such as requesting, querying, and transporting data.
- We conducted practical testing to implement the proposed system, assessed the system's security, and evaluated its performance, cost, and latency.

2 Related Works

2.1 Cross-chain Technology

In the recent study, [4] provided a comprehensive overview of cross-chain interoperability technologies, encompassing notary mechanisms, sidechains/relays, hash-locking, distributed private key control, and others. These technologies aim to enable the transmission of data and transactions between different blockchains, which is a critical requirement for the widespread adoption of blockchain technology. [5] proposed a quantum-secure notary scheme for resilient cross-blockchain transfers and [6] introduced a notary group mechanism providing enhanced security guarantees. [7] focuses on atomic cross-chain swaps via hash-locked contracts, enabling trustless asset exchange. Unique solution like Cosmos [8] connects heterogeneous chains via relay bridges, with collective validation by multiple parties for robust trust. While progress has been made, blockchain interoperability remains an open challenge. Constructing a multi-chain interoperable data system, especially for healthcare, faces several challenges. One key issue is integrating different blockchain structures, each with its unique rules. Ensuring security and privacy is crucial, aligning with healthcare regulations adds complexity. Another challenge is maintaining data integrity across various chains. For instance, patient records scattered in different hospital blockchains need an efficient system for better management. These challenges highlight the need for a robust and flexible multi-chain data system for effective healthcare applications.

2.2 Identity management systems & Decentralized identifiers

Identity management (IdM) is defined as policies, rules, methods and systems that implement identity authentication, authorization management, access control, and operation audit based on digital identity [9]. The centralized identity model stands as the most traditional approach, however, this model carries inherent limitations, such as privacy concerns, escalating data volumes, and the growing ubiquity of online accounts that individuals must juggle, each demanding vigilant safeguarding [10]. The federated identity model has emerged as a salient solution to the quandary of managing numerous disparate accounts. Users can leverage identity credentials established within one security domain to gain access to various other sites and services. Notably, OAuth and OpenID Connect constitute instrumental standards within the realm of federated identity protocols and are widely used in today's web services [11]. Extensive efforts have been devoted to developing user-centric IdM, emphasizing improvements in both user experience and security. CardSpace, a product developed by Mircosoft, has applied the user-centric identity model. In consonance with this trajectory, Lenz et al. [12] proposed a lightweight model for user-centric and qualified identity information that facilitates selective disclosure and domain-specific altering of single identity attributes in order to protect the citizen's privacy.

Contemporary IdM paradigms often employ a centralized model, wherein specific organizations assume responsibility for issuing and managing user IDs, resulting in user dependency and limited control over identity data. Decentralized Identifiers (DIDs) have emerged as a promising alternative, offering users enhanced autonomy and control over their identity information, and reducing reliance on centralized identity providers. A seminal work in [13] delves into the profound impact of DIDs on the evolution of data exchanges, offering a comparative analysis that underscores the distinctions between DIDs and their centralized counterparts. The study conducted by [14] introduces a robust registration and authentication mechanism, ingeniously utilizing a double-layer blockchain architecture that seamlessly incorporates DIDs. [15] aligns with the World Wide Web Consortium (W3C) DID recommendation [16], signifying the growing adoption of DIDs as a critical element in the contemporary IdM landscape.

3 Proposed System

In the healthcare domain, hospitals have embraced blockchain networks for managing personnel, patients, and EMRs. However, a pressing need arises to enable seamless data exchange across disparate hospital networks, enhance identity management for hospital entities, establish connections between EMRs and their owners, and enable efficient data inquiries across multiple EMRs and hospitals. To address these challenges, we introduce MIDAS as the central component of our architectural paradigm (Fig. 1). MIDAS acts as a Sidechain, facilitating interoperability between heterogeneous blockchain networks. This architecture effectively fulfills the aforementioned requirements while prioritizing the security, efficiency, and confidentiality of personal information within participating blockchain networks. Assume that the Doctor belongs to Hospital A, and needs to access EMRs within the hospital or access other EMRs located inside or outside the patient's existing hospital. For Hospital N where the patient went and owns EMR in both Hospital A and N. The hospital system is implemented with the following roles: Doctor and Patient.

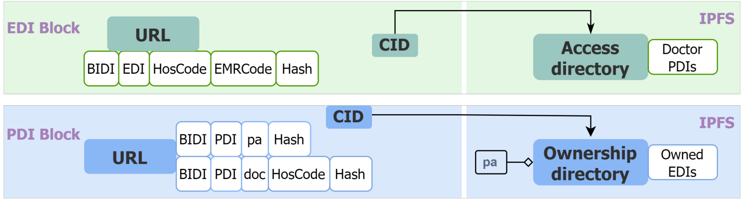

Fig. 2. The architecture for configuring and storing BIDI in MIDAS and IPFS.

3.1 BIDI - Blockchain Interoperability Decentralized Identifier

BIDI is designed to identity provisioning and enable smooth interactions between different blockchain networks, applicable and versatile across various subjects within our scope. Each participant in this system, including Doctors, Patients, and EMRs, possesses a distinct and unambiguous identification marker, represented by a URL-based identifier. The URL-based identifier consists of three essential components, as illustrated in Fig. 2.

1. **BIDI:** The fundamental prefix following it is types of BIDI encompassing EMR - EDI and Person - PDI.
2. **Specific Identifier Path:** As shown in Fig.2, the structure of the Path is contingent upon *Type* of BIDI and *Role*. In the case of the EDI type, it comprises the following components: *HosCode*, signifying the unique identifier of the hospital to which the EMR is affiliated; *EMRCode*, representing the distinctive EMR code; and *Hash* string. Conversely, the PDI type encompasses distinct components, including roles such as *doctor* or *patient*. Additionally, *HosCode* is included if the role is doctor, signifying the hospital to where they belong. Finally, a *Hash* string, calculated from the Public and Private key pair.

BIDI directory is a dataset designed to encompass predefined information crucial for establishing data linkage management and automated data access control. It is linked to URLs associated with the same BIDI, with different types of BIDI having their distinct directory variants. For EDI-type BIDIs, each EDI possesses an Access directory. This Access directory contains PDIs, with the top and mandatory PDI corresponding to the URL of the patient who is the rightful owner of the corresponding EMR. Subsequent PDIs pertain to doctors sharing the same HosCode as the EDI, thereby granting them seamless access automatically to the EMR's contents. The management of the Access directory, encompassing tasks such as addition or removal of DocPDIs, is entrusted to the patient who is the owner of the EMR. Conversely, for PDI, only the patient role is endowed with an Ownership directory. Within this directory lies a comprehensive record of EDIs corresponding to EMRs owned by the patient, creating pivotal links between data entities and expediting data retrieval. As a result, an inventory of EMRs is curated, affording patients the discretion to select from this catalog for viewing or sharing with doctors.

3.2 MIDAS - Multi-chain Interoperable Data and Access System

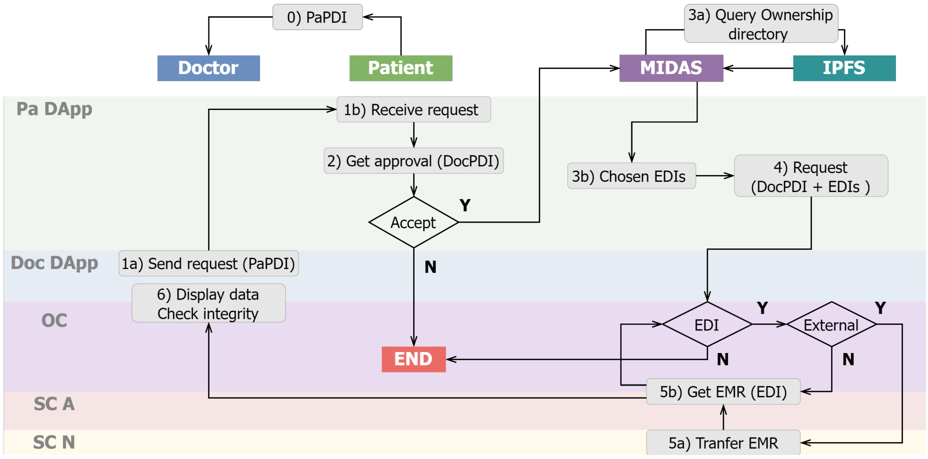

Fig. 3. EMR access request processing flows across multiple sources

MIDAS plays a role similar to that of Sidechain in cross-chain solutions, acts as an intermediary, facilitating communication between different blockchains. As a decentralized oracle network, MIDAS inherits and encapsulates the diverse capabilities of blockchain oracle technology. It establishes a bidirectional connection between smart contracts on the blockchain network and the external world. Additionally, MIDAS serves as the repository for BIDIs, and its organizational structure adheres to a designed schema. Each BIDI is stored in a distinct block, following the data model depicted in Fig. 2.
Owing to the inherent characteristics of MIDAS, which features an architecture akin to that of a blockchain and is ill-suited for the storage of mutable data such as BIDI directories, a strategic amalgamation with InterPlanetary File System (IPFS) has been orchestrated. The integration with IPFS serves as the repository for these dynamic datasets. To establish matching between the BIDI directory and its corresponding URL stored within MIDAS, a pivotal step necessitates affixing a unique IPFS hash (CID) to the URL. Consequently, when interfacing with a BIDI stored within MIDAS, users can seamlessly initiate queries that retrieve the associated directory from IPFS.

3.3 Data authorization mechanism

Algorithm 1 EMR access request procedure

```
$PaDApp \leftarrow$ SendEMRrequest $\leftarrow DocDApp$                ▷ Step 1
$EMRreq(DocPDI) \leftarrow PaPDI$
if getApproval($DocPDI$) then                                         ▷ Step 2
    $ODir \leftarrow CID, PaPDI$                                      ▷ Step 3
    $ListEDIs \leftarrow ODir$
    $sum \leftarrow ChosenEDIs \leftarrow$ ChooseEMRs($ListEDIs$)
create Fetch data Request $\leftarrow DocPDI, ChosenEDIs$             ▷ Step 4
    $i \leftarrow 0$
    while $i \neq sum$ do                                             ▷ Step 5
        $EDI \leftarrow ChosenEDIs[i]$
        if DocPDIHosCode $\neq$ EDIHosCode then
            Crosschain Data transfer $\leftarrow EDI, DocPDI$
        end if
        $i \leftarrow i + 1$
        Display data for doctor $\leftarrow$ getEMR($EDI$)
    end while
end if
END
```

The data transfer activities within the system are depicted in Fig.3. The process of a Doctor sending access requests to a patient's existing EMRs unfolds as follows: **Step 0)** Doctor first obtains the patient PDI. **Step 1)** Via the Doc DApp, Doctor specifies PaPDI and sends a data access request to DApp of patient. **Step 2)** Get the approval. **Step 3)** PaDApp retrieve the corresponding Ownership directory on IPFS. It compiles a list of EDIs from which the patient selects EMRs to share with the Doctor. **Step 4)** Create a query request and sends it to MIDAS. **Step 5)** Check EDI quantity, HosCode and then get the requested data. **Step 6)** Display EMRs to the Doctor and data integrity can be verified through URL hash string. The operation subsequently reverts to step 5. Also, algorithm 1 provides a succinct representation of this operation sequence. **Algorithm 2** outlines the automated authorization process for granting data access permissions to Doctors. The process begins when the Doctor sends the EDI requiring access to the EMR. The DApp performs an initial verification by comparing the HosCode in the DocPDI with that of the requested EMR. Next, the DApp interfaces with MIDAS, creating an oracle contract to search for the corresponding EDI block. If the EDI block exists, a query is sent to the Ownership directory stored in IPFS. The query aims to confirm the presence of DocPDI within the directory, verifying the Doctor's authorization to access the specific EMR. If the verification process succeeds, the Doctor's access request is approved, and then transmit the required data to the Doctor.

Algorithm 2 Automatic data access control mechanism

```
SendEMRrequest ← $DocPDI, EDI$                          ▷ Step 1
if DocPDIHosCode == EDIHosCode then
create Oracle contract
    Query ADir ← $EDI, CID$                             ▷ Step 2
    if isDocPDIexist($DocPDI$) ← $ADir$ then            ▷ Step 3
        getAccess                                       ▷ Step 4
    end if
end if
END
```

4 Experiment Results

In this section, we evaluated the practical performance of the proposed system by implementing and deploying Quorum, Ethereum and MIDAS, also conducted experimental transactions including: Registering entities with the DApp, storing new EMRs in the hospital's IPFS storage, automating the EMR sharing process internally using BIDI and manually selecting EMRs to share. Table 1 provides a detailed breakdown of the specific activities of each transaction and presents time consumption and the cost results in terms of gas and USD for each of them. We also performed multiple measurements for each experimental transaction to ensure the maximum accuracy and reliability of the figures. Based on the obtained results, we evaluate the cost of sharing EMR data across the blockchain as relatively low, dependent on the complexity of the data. On the other hand, the cost of storing new BIDI is relatively higher due to the many complex steps involved, however, this process only needs to be done once. Importantly, the cost for the creation and update of the BIDI directory is quite low, demonstrating the efficiency of the system's permissions function. Overall, the experimental results we achieved are relatively favorable. Therefore, we assess that our proposed solution has shown positive results and further development potential.

Security is a paramount consideration in the architecture of our system, featuring notable focal points. Firstly, MIDAS is a decentralized oracle network, and each transaction is verified by all Oracles, ensuring transparency and preventing fraudulent activities. Secondly, BIDI provides identity and permission for entities in the blockchain, ensuring that only authorized individuals can access the data, thus making the system resilient against data breaches and ensuring data privacy. Notably, BIDI adopts a public URL format devoid of sensitive data, mitigating the risk of exposing personal information. Lastly, extends comprehensive data management and access capabilities to data subjects. Consequently, the system is adept at aligning with diverse healthcare regulations across global jurisdictions, and compliance with standards such as HIPAA (United States), GDPR (EU), and PHIPA (Canada). This adaptability becomes particularly salient when considering the system's prospective global deployment and application within the healthcare domain. Moreover, BIDI finds application in a myriad of healthcare scenarios, exemplified by real case applications such as EMR Management, Cross-Border Medical Consultation, Decentralized Clinical Trials, Collaborative Medical Research, and Emergency Patient Data Access.

Table 1. The average cost consumption of transaction

Transactions	**Gas**	**USD**	**Seconds**
Deploy Smart Contracts	2,365,536	227.13	
Register Doctor	111,476	10.70	1.62
Register Patient	202,711	19.46	1.82
Create new EMR	152,673	14.66	2.51
Internal automatic request	12,774	1.23	0.93
Overall Request	330,888	31.77	19.97

5 Conclusion

In this research, we have introduced MIDAS system integrated with our decentralized identity management solution, BIDI scheme. Our objective is to enhance the capabilities of the healthcare sector by overcoming traditional barriers to data management and access. The system provides a secure and efficient framework for cross-chain data transfer, enabling seamless interoperability. It also enables decentralized administration of entity identities, aligning with contemporary data governance practices. The BIDI directory is a breakthrough mechanism that grants autonomous data access control and establishes associations with rightful owners, enhancing user experience and query efficiency. We have rigorously tested the practical viability and effectiveness of our proposal through various scenarios, validating its robustness and foreseeing its promising applications in the healthcare domain. Moving forward, our future research endeavors will focus on fortifying the privacy and security measures surrounding medical data, while concurrently striving to optimize the cross-chain system by minimizing latency and cost.

Acknowledgment

This research is funded by the Faculty of Computer Networks and Communications, University of Information Technology, Vietnam National University Ho Chi Minh City, Vietnam.

References

1. Yan Pang. A new consensus protocol for blockchain interoperability architecture. *IEEE Access*, 8:153719–153730, 2020.
2. Thomas Hardjono, Alexander Lipton, and Alex Pentland. Toward an interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management*, 67(4):1298–1309, 2019.
3. Christopher G Harris. Cross-chain technologies: Challenges and opportunties for blockchain interoperability. In *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, pages 1–6. IEEE, 2023.
4. Wei Ou, Shiying Huang, Jingjing Zheng, Qionglu Zhang, Guang Zeng, and Wenbao Han. An overview on cross-chain: Mechanism, platforms, challenges and advances. *Computer Networks*, 218:109378, 2022.
5. Haibo Yi. A post-quantum blockchain notary scheme for cross-blockchain exchange. *Computers and Electrical Engineering*, 110:108832, 2023.
6. Anping Xiong, Guihua Liu, Qingyi Zhu, Ankui Jing, and Seng W Loke. A notary group-based cross-chain mechanism. *Digital Communications and Networks*, 8(6):1059–1067, 2022.
7. Maurice Herlihy. Atomic cross-chain swaps. In *Proceedings of the 2018 ACM symposium on principles of distributed computing*, pages 245–254, 2018.
8. Jae Kwon and Ethan Buchman. Cosmos whitepaper. *A Netw. Distrib. Ledgers*, page 27, 2019.
9. Yuan Cao and Lin Yang. A survey of identity management technology. In *2010 IEEE International Conference on Information Theory and Information Security*, pages 287–293. IEEE, 2010.
10. Oscar Avellaneda, Alan Bachmann, Abbie Barbir, Joni Brenan, Pamela Dingle, Kim Hamilton Duffy, Eve Maler, Drummond Reed, and Manu Sporny. Decentralized identity: Where did it come from and where is it going? *IEEE Communications Standards Magazine*, 3(4):10–13, 2019.
11. Daniela Pöhn and Wolfgang Hommel. An overview of limitations and approaches in identity management. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pages 1–10, 2020.
12. Thomas Lenz and Vesna Krnjic. Towards domain-specific and privacy-preserving qualified eid in a user-centric identity model. In *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)*, pages 1157–1163. IEEE, 2018.
13. Yoshiaki Fukami, Takumi Shimizu, and Hiroyasu Matsushima. The impact of decentralized identity architecture on data exchange. In *2021 IEEE International Conference on Big Data (Big Data)*, pages 3461–3465. IEEE, 2021.
14. Xuehan Li, Tao Jing, Ruinian Li, Hui Li, Xiaoxuan Wang, and Dequan Shen. Bdra: Blockchain and decentralized identifiers assisted secure registration and authentication for vanets. *IEEE Internet of Things Journal*, 2022.
15. Sandro Rodriguez Garzon, Hakan Yildiz, and Axel Küpper. Decentralized identifiers and self-sovereign identity in 6g. *IEEE Network*, 36(4):142–148, 2022.
16. Drummond Reed, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, Markus Sabadello, and Jonathan Holt. Decentralized identifiers (dids) v1. 0. *Draft Community Group Report*, 2020.