International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 10, No. 3, 2023, pp. 1-6.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Blockchain-oriented Digital Identity Management for Secure Online Transactions

Ishita Rao [a], Pradeep Joshi [b]

[a] *Ishita Rao, Visual Computing Division, Patna School of Informatics, India.*
[b] *Pradeep Joshi, Visual Computing Division, Patna School of Informatics, India.*

Abstract

Financial organizations are adopting an Open Bankings (OB) pattern for creativity in services and incorporation. OB permits Third-Party Servicing Providers (TSPs) to entry consumer financial data to identify optimal offers and enhance customer service. The reliance on third parties essential for the functioning of the OB environment prompts inquiries about digital identity incorporation, information exchange, and the safeguarding of secrets. Distributed Applications (DApps) for data classification and secret protection, user consent capturing, tracking TSP accessibility actions, controlling Applications Programming Interfaces (APIs), and maintaining Self-Sovereign Identity (SSI) are available; however, they have not yet been incorporated into a functional three-phase OB strategy. Upon evaluating the principal needs of main OB users, the research formulated a Blockchain-oriented Identity Managing and Access Controlling System (BIMACS) that incorporates benefits from both conventional banking and blockchain-based technologies. The BIMACS facilities utilize smart agreements and an undocumented authenticating system to establish a transaction security management system, which provides features such as distributed Third-Party Logins (TPL), OB account creation, information authorization, incorporated transactions, and TSP access tracking. The system efficiency study's findings demonstrate that the suggested structure's frequently executed functions incur a lower computational price than the median operations price on open Ethereum.

Keywords: Blockchain, Identity Management, Security, Transactions

DOI: 10.71086/IAJSE/V10I3/IAJSE1023
Received: 12 June 2023/Revised: 17 July 2023/Accepted: 07 August 2023/Published: 28 September 2023

Introduction

A fundamental objective of Open Banking (OB) is to guarantee agreement when disseminating consumer financial information to other entities [1]. Financial institutions provide Application Programming Interfacing (APIs) to Third-Party Servicing Providers (TSPs) to develop new solutions, data analysis, and economical services designed to enhance client experiences [2]. OB is thought to facilitate client demands, and TSP development is focused on uncovering supplementary client requirements and expediting monetary inclusion. A critical concern is safeguarding the confidentiality of funds, investments, loans, account details, and other Personal Information (PI) forms [3]. Banks are apprehensive about the risk of fraudulent transactions and account tampering by hackers when releasing APIs to TSPs.

Blockchains (BC), which are distributed electronic registers that save documents or information in securely connected barriers, can safeguard the incorporation of information and client confidentiality by regulating access, securing operations, and ensuring that information is tamper-proof [4]. This facilitates secure usage in "trustless" conditions—tasks that do not need reliance on others. The Ethereum distributed ledger platform facilitates autonomous application installation and interactions using Smart Contracts (SCs) within its network [5]. It has been proposed that integrating SC-based variable access controls in forthcoming data-sharing platforms can alleviate users' inability to modify their approvals. The tamper opposition, openness, and verification attributes of BCs provide solutions to worldwide operational business difficulties related to harmful assaults, theft of identities, leakage of information, and privacy breaches, among others.

To effectively resolve these issues, the research presents the solution for a complete BC-based Identity Managing and Access Controlling System (BIMACS) architecture for the OB ecosystem. BIMACS comprises 3 components: (a) a Dependent Co-Governanced Model (DCGM) that establishes an interoperating back-end for regulatory authority and banking cooperation, selecting choices, and participants' authorization; (b) a Distributed Identities Integrating Model (DIIM) that offers enhanced privacy-preserving features compared to user-based identity administration models such as those utilized for Facebook authentication or the search engine IDs; and (c) a Distributed Access Controlling Model (DACM) for granting or rescinding consumer information permissions for various third sectors.

The research employed these components to create six features that fulfill the specifications of the Personal Information Transactional Safe Controlling (PITSC) system. BIMACS effectively resolves a fundamental incompatibility between conventional banking practices and public BCs by incorporating an international BC network that guarantees privacy in real-name registrations while maintaining openness regarding anonymous transactions.

Background

The research confines the discourse to the technologies and designs that advocate for personal data governance through BC technology [6]. BC technology continues to develop, and the quantity of BC apps is gradually rising. The utility of the BC system for private information administration remains inadequately investigated. A pioneering effort in this area involved the development of a protocol that transforms a BC into a computerized access-control manager for a decentralized private information management platform [7].

The proposal involves using auditable contracts on BC technologies to ensure open access to and handling of private information by data owners while maintaining a privacy-preserving design. A methodology is provided for gathering internet identity and reputational data based on a social dependence system to deliver online behavioral ratings.

Numerous studies in medicine have investigated using BC to access health information. A significant and pertinent contribution was made when the researchers suggested a structure utilizing artificial intelligence and BC technology to empower individuals with ownership over their private records, mainly medical information. A decentralized record administration system utilizing BC software for handling electronic medical records has been suggested. The study presented a mobile application design utilizing BC technology to empower patients to own, manage, and share their information effortlessly and securely while maintaining privacy. The study introduces a novel theoretical framework and system structure for human-centric private information and authentication, aligned with responsibility, utilizing BC and SC, in contrast to prior studies.

Proposed BC-based Identity Managing and Access Controlling System

Fig. 1 illustrates that the primary objective of BIMACS is to partly distribute the environment backbone presently managed by the Financial Data Service Companies (FISC), thereby converting it into an infrastructure that a Regulatory Authority (RA) and financial organizations control. BIMACS is utilized to create a BC-oriented PITSC system for OB.

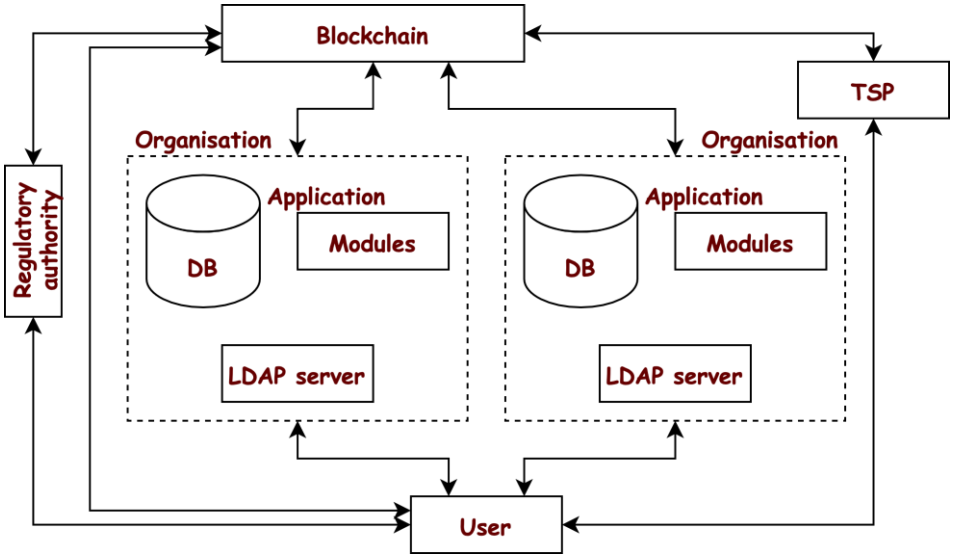


Fig. 1: Architecture of the Proposed System

The secondary objective is to develop a App that enables consumers, Financial institutions, TSPs, and RAs to utilize different features of the OB environment for consortia BC co-control, user authentication incorporation, secured information communication, and further capabilities. The third objective is to employ BC and related system technologies to address the needs of the 4 primary OB players while fulfilling all three OB stage's necessities: open product data inquiries, account data integration, and payment authorization.

3.1 Implementation

The research employs the Model-View-Controller (MVC) architecture within the OB environment to conceptualize and construct the PITSC system grounded in BIMACS. Fig. 2 illustrates the PITSC construction, with four levels: performance, network accessing, infrastructures, and financial information levels. Customers' personally identifiable and financial information is stored locally on the banks' client and database. The BIMACS architecture is the foundational layer applicable to many situations with analogous secure data-sharing needs.

The three supply chain managers, along with other pertinent components, can constitute three primary modules to establish the basic framework of BIMACS:

DCGM: This module oversees the operation of the distributed database, co-governance of nodes, handling of involvement, formulation of data access control policies, and administration of open API administration, among other functions.

DIIM: They offer a more privacy-preserving Self-Sovereign Identification (SSI) than user-centric identification management systems such as Facebook Authentication or Google Identity.

DACM: It is intended for consumers to autonomously control or cancel information accessing control permissions for various outside parties.

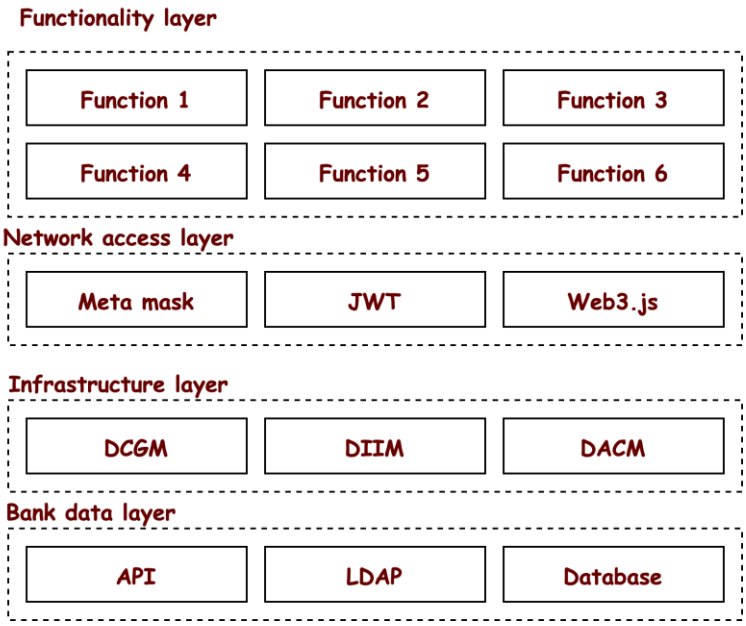


Fig. 2: Layered Architecture

Applying tools within the network access level, the PITSC system encompasses six features to fulfill the scenario's needs. For straightforwardness, the research frequently employs the term BIMACS instead of PITSC, as this paper exclusively focuses on modeling BIMACS within the OB situation. The subsections will elucidate the six capabilities, design concepts, and comprehensive methods.

Results

The analysis delineates three roles related to account integrating (write actions that will alter bright contract states on-chain), with their efficacy test outcomes depicted in Fig. 3. The length of a transaction encompasses the time used for advertising to the whole BC system, confirmation by miners, and the publication of the resultant blocks to the ledger. The throughput will fluctuate due to the intricacy of the SC condition transition. Fig. 4(a) illustrates that a simpler code correlates with increased throughput, indicating that more operations are handled within similar blocks. The disparity seen among bind-Account and other methods in finding was substantial; bind-Account processes around 5 transactions per second (tps) (the BC system can accommodate only five account binds per second). The legally binding process necessitates the creation of new agreements (ACMgr), resulting in increased gas costs. Each user must do SSI-binding only once to ensure adequate efficiency.



Fig. 3: Throughput Analysis

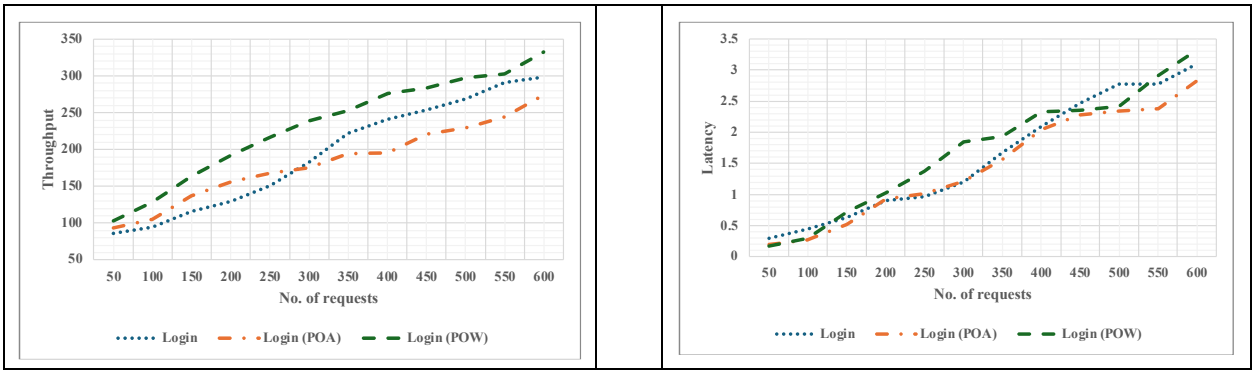


Fig. 4: Throughput and Latency Analysis

Fig. 4(b) illustrates the outcomes of the login performance evaluation. The conventional login process involves the consumer submitting an authentication need containing login credentials and passwords to the server for verification. The research evaluated distributed TPL utilizing two distinct agreement methods: Login(POA) and Login(POW). Regarding the Login operation, there is minimal difference between the two agreement techniques. The findings indicate that the login efficiency of all three approaches is comparable at transmission rates below 300 tps.

In contrast, the conventional login method outperforms the others at rates beyond 300 tps. The results indicate that original authentication exhibits reduced delay, which is intuitive. In essence, there is minimal difference among Login(POA) and Login(POW) as both are reading actions that do not alter the SC condition. These distributed TPLs exhibit less efficiency than conventional Logins, yet they adequately fulfill login requirements.

Conclusion

This article presents the idea for a BIMACS structure that incorporates the benefits of conventional banking and BC innovation grounded in a thorough analysis of OB demands, online identity managing structures, authentication processes, information-sharing necessities, and access controlling strategies. The structure is developed to address the issues related to many online identities and the necessity of overseeing other parties' utilization of private data. The research tackled the operational company demands for safely delegating access rights to information and delivering secure application development connectors.

BIMACS amalgamates the benefits of conventional banking practices with BC-based technology, thereby enhancing the capacity for adherence to all rights and technical stipulations. The suggested BC-based SSI solutions are managed by a group of RAs and financial institutions, although it applies to non-OB uses. One of the forthcoming objectives is to enhance BIMACS by incorporating cross-ecosystem cooperation and security administration, as well as to execute pilot tests focused on developing a more robust system for anticipated metaverse apps inside the framework of Web 3.0.

References

Tenfelde, S. M., Hatchett, L., & Saban, K. L. (2018). “Maybe black girls do yoga”: A focus group study with predominantly low-income African-American women. *Complementary therapies in medicine*, *40*, 230-235. https://doi.org/10.1016/j.ctim.2017.11.017

You, C. (2022). Half a loaf is better than none: The new data protection regime for China's platform economy. *Computer Law & Security Review*, *45*, 105668. https://doi.org/10.1016/j.clsr.2022.105668

Usman, M., & Qamar, U. (2020). Secure electronic medical records storage and sharing using blockchain technology. *Procedia Computer Science*, *174*, 321-327. https://doi.org/10.1016/j.procs.2020.06.093

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(11), 2266-2277 https://doi.org/10.1109/TSMC.2019.2895123.

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156-174. https://doi.org/10.1080/17579961.2020.1727094

Mukherjee, P., & Pradhan, C. (2021). Blockchain 1.0 to blockchain 4.0—The evolutionary transformation of blockchain technology. In *Blockchain technology: applications and challenges* (pp. 29-49). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69395-4_3

Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., ... & Rahman, M. H. (2021). Blockchain and artificial intelligence technology in e-Health. *Environmental Science and Pollution Research*, *28(38)*, 52810-52831. https://doi.org/10.1007/s11356-021-16223-0