Secure Private Blockchain-Based Instant Messaging Platform for Social Media Services

Marc Jayson Baucas, *Member, IEEE*, and Petros Spachos, *Senior Member, IEEE*

***Abstract*—Social media services enable global communication via instant messaging (IM) platforms. However, their widespread usage has resulted in server regulation issues because most are centralized, while they also pose privacy concerns due to endpoint-based security vulnerabilities. In response, we present a private blockchain-based IM platform that utilizes blockchains to secure data through immutability. We implement it in a RESTful Application Programming Interface (REST API) Web server for better load balancing compared to the centralized IM architectures via decentralization. We further implement end-to-end encryption (E2EE) using public-private key pairs to improve data privacy. We evaluated the proposed design by highlighting its advantages over centralized IM platforms.**

***Index Terms*—Messaging platform, Internet of Things, blockchain, decentralization, end-to-end encryption.**

I. Introduction

SOCIAL media services for instant messaging (IM), such as Messenger and WhatsApp, are among the most popular platforms for global communication. They allow long-distance communication and media sharing. However, the widespread usage and volume of data they handle daily causes most services to run into management issues due to centralization [1]. At the same time, they pose privacy concerns since central servers hold a majority of message data, presenting confidentiality issues [2].

We propose permission blockchain technology to address these issues in centralization and data privacy. Blockchains are known for their decentralization and immutability [3], two characteristics that can reduce these concerns in current IM platforms. Their decentralized architecture can lower the risk of targeted attacks. Also, their immutability can employ tampering resistance, creating a more secure and reliable messaging system for users to be comfortable using. In addition to the advantages of blockchain through its security features, we further enhance security with a public and private key pair to enable end-to-end encryption (E2EE) within the IM platform.

Manuscript received 2 February 2024; accepted 30 March 2024. Date of publication 10 April 2024; date of current version 31 May 2024. This work was supported in part by the Natural Sciences and Engineering Research Council of Canada under Grant RGPIN/2016-04007. The associate editor coordinating the review of this article and approving it for publication was M. Erol-Kantarci. *(Corresponding author: Petros Spachos.)*

The authors are with the School of Engineering, University of Guelph, Guelph, ON N1G 2W1, Canada (e-mail: baucas@uoguelph.ca; petros@uoguelph.ca).

Digital Object Identifier 10.1109/LNET.2024.3386974

II. Background

A. Current State of IM Platforms in Social Media Services

This generation emphasizes the significance of social media services, and many industries have incorporated them into their services [4]. Specifically, IM platforms have become a crucial component of the lifestyle of many individuals globally. Some are utilized for communication and data sharing among peers, resulting in a global network of information in many different forms. Larger decision-making bodies, such as government and business administrations, use IM platforms such as Messenger, Slack, and WhatsApp for most conversations on decisions and meeting notes. Even in the most private units, IM services within Instagram, TikTok, and X/Twitter record every personal end-to-end communication, from messages to shared media. In [5], they use it for monitoring non-severe COVID-19 patients in isolation programs during crises. They integrated it with LINE, an existing messaging application, to assess patient health and notify practitioners of high-risk scenarios through a chatbot. Other implementations capitalize on using the messaging service for alerting users. In [6], they implement a road monitoring system that notifies users of road emergencies through a centralized vehicular network.

However, its incorporation into many industries presents concerns due to the volume of data these networks hold. The first is for proper data control and management due to the centralized nature of most IM platforms [7]. As a result, it becomes a vulnerability for targeted attacks to disrupt services and steal information, making data ownership a point of contention. The second concern is the security and privacy issues due to the volume of data managed by each social network [8]. These platforms share valuable information, so data leakages are a legitimate concern for its users. Data must be secure from malicious attacks attempting to obtain or modify them illegally. Blockchain technology is a promising approach to address these issues.

B. Private Blockchain Approach

A blockchain is a list of cryptographically-linked blocks of [9]. Its decentralization allows the distribution of data control, alleviating the burden towards a single server and reducing the risk of significant data loss [10]. Blockchain design benefits IM platforms by addressing data usage and control concerns. Aside from their usage, blockchains can address privacy issues. The blockchain creates a tamper-proof data structure using cryptographic techniques and immutability [11]. As a result, it can protect user's data. Blockchains have positively impacted and advanced other industries such as healthcare, finances, and supply chains [12]. Therefore, IM

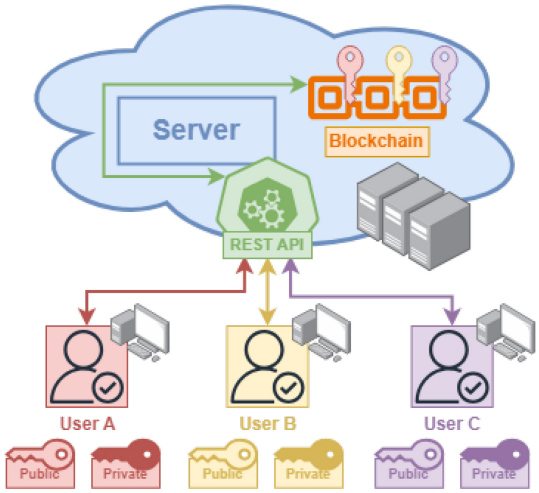

Fig. 1. The platform's network hierarchy and other components of its design.

Fig. 2. Screenshot of a login attempt through the login page using test credentials.

TABLE I
LIST OF REST API REQUESTS TO ACCESS FROM THE WEB SERVER

Requests	Method	Description
/check	GET	It checks if the user logged into the web page still has a valid session.
/login	POST	It verifies the provided login credentials and if a session exists.
/logout	POST	It logs out the current user session
/friendslist	POST	If the user is valid and logged in, it responds with their friend list.
/messages	POST	If the user is valid, logged in, and friends with another account, it responds with the message history.

Fig. 3. Screenshot of the home page using a test account displaying messages.

platforms within social media services are an area with the potential to improve.

Our approach differs from other blockchain implementations as we suggest using private blockchain to create a more exclusive and low-cost platform. Private blockchains provide a trusted and private data structure with low transaction costs without the Proof-of-Work (PoW) and fewer participating nodes due to its exclusivity [13]. Also, most frameworks collaborate with existing IM platforms and designs to create a working system. We plan to use blockchain technology with our RESTful Application Programming Interface (REST API) design to build a locally deployable, low-cost alternative for small groups to use, ensuring their conversations and messages are secure and under their control within their local area networks. Therefore, we propose a secure IM platform using private blockchain technology partnered with a REST API Web service and E2EE system, giving better control for users over their messages and shared data.

III. Platform Overview and Design

A. Overview

We introduce a private blockchain-based IM platform that promotes data privacy and decentralization. It utilizes the immutable and tamper-proof advantages of blockchain technology to reinforce the security of user information. Next, we use a REST API Web server to manage the blockchain and the incoming and outgoing data from the server. It uses its load-balancing aspect to regulate the endpoints while managing the blockchain. Then, we incorporate public-private key pairs to implement E2EE, reinforcing user message privacy within our platform. A diagram showing the platform's network hierarchy and other aspects of its design is in Fig. 1.

B. Components and Design

1) Frontend Design: The front end is a Web browser interface using ReactJS and NodeJs. We selected it due to its well-detailed documentation and massive developer community for support, allowing us to utilize it effectively. The website's architecture consists of a login and home page. The login page will allow users to enter the IM service using valid credentials. A screenshot showing the login page with test credentials is in Fig. 2. A home page will display the account details and messages of the logged-in user. A screenshot showing the home page with a test account logged in is in Fig. 3. In the case of a logged-in user, they can select a friend through the home page and communicate it to the REST API server. If the server verifies their connection, it will send their message history for the user to view through the web page.

2) Backend Design:

a) REST API: The REST API design uses Flask as its Web framework. Its Python-based code structure and minimal requirements for additional libraries made it a favourable option. We designed the Web server to contain corresponding requests to provide requested information such as account details, friend lists, and message histories to the front end. A list of all these REST API requests and their functions is in Table I. Also, we designed the Web server to manage the login

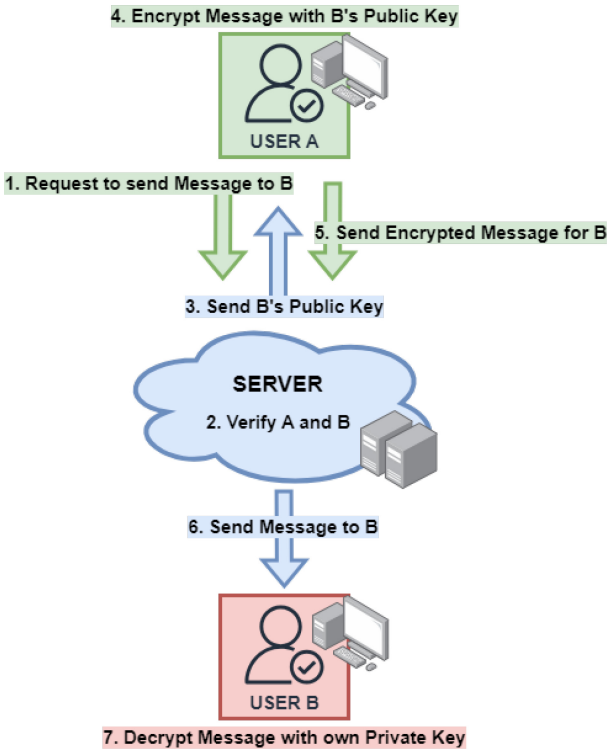

Fig. 4. E2EE implementation in our proposed platform using the blockchain and public-private key pairs.

sessions to ensure that all requests are valid to keep the user data secure. It consults an initialized blockchain to verify every request it receives to guarantee that it responds accordingly to known and malicious users.

b) Private blockchain: We coded the private blockchain in Python to store the user's messages and other information. The REST API Web server will consult it to verify all incoming requests. Its structure consists of two classes: the block and the chain. The block class consists of an ID, a timestamp of its creation, a list of data entries, a hash of the previous blockchain iteration, a list of smart contracts, and a nonce. Each entry within the block class is a Python dictionary containing keys depending on the type of information it holds. The entry types our design currently handles are user accounts, friend lists, and messages. The chain class manages the generation and connection of blocks, creating the blockchain. We initialize it along with the deployment of the REST API Web server. We implemented the access control system through the blockchain by checking the source of every incoming message and request. If the user is valid, the server grants access to it. This system achieves security and confidentiality by protecting existing users' data from being accessed by malicious devices. As a result, the Web server keeps information secure and conversations private through this access layer.

c) End-to-end encryption: We implemented the E2EE aspect of the design by incorporating public-private key pairs in encrypting messages between users. Upon registering, we programmed the Web application to generate a public and private key pair through a Secure Hash Algorithm 256-bit (SHA256) library in Python using Advanced Encryption Standard (AES) encryption. The private key will remain known only to the device where the user logs in from. As for the public key, the user's device will send it to the server for storage. When a known user sends a message, it expresses its intent to the server. The server will first verify that the source and destination are valid accounts. If so, it will respond with the destination's public key. This user, expressing intent to send the message, will encrypt it with that key and forward it to the server. The server acts as the middleman. Note that it is to see the message's contents, as only the private key holder can decrypt it. The receiving user will then decrypt it with their private key. A diagram showing the different steps of the E2EE system at work is in Fig. 4. This flow of operations promotes user privacy within our platform as it keeps the contents of messages accessible only to the users.

TABLE II
COMPARING OUR PROPOSED DESIGN AGAINST EXISTING IM PLATFORMS

Aspect to compare	Centralized IM Platforms	Proposed platform
Data Storage	Most have centralized storage.	Achieves decentralization via a web server and private blockchain.
Tamper Resistance	Harder to detect tampering with only one verifiable basis.	Multiple distributed copies of the blockchain make modifications and anomalies easier to detect and address.
User Privacy	Without E2EE, data is visible to anyone with administrative access.	Having E2EE keeps data encrypted and secure. Only the holder of the private key can decrypt their messages.
Data History Reliability	Anyone with administrative access can tamper with the data.	Cryptographically linked blocks and decentralization promote reliability through immutability.
Network Service	The centralized server makes it more likely to experience downtimes through overloading.	The decentralization via the REST API web server and private blockchain creates a distributive architecture, ensuring proper load balancing.

IV. RESULTS AND EVALUATIONS

A. Resulting Platform

Our proposed platform and design resulted in an IM Web application utilizing private blockchain technology as its data storage to reinforce security. Also, it incorporates private key encryption, implementing E2EE, and improving data privacy for its users. The code is fully deployable using NodeJS. Anyone accessing the same WiFi network as the local host can connect to the website through any Web browser. However, only those registered to the blockchain can log into the IM platform and use its service. Since it is a private blockchain, there is no need for any further subscription or a cryptocurrency wallet. All you need to do is register an account within

the private blockchain. It is also possible to send messages, with every message stored within the blockchain. As a result, we have a working testbed that can simulate our platform.

For device complexity, our design uses IoT devices. It has no high processing requirements. However, it must still have a capable interface to display the messages and manage the REST API requests and responses. Also, as long as the device can run Python scripts, it can manage the E2EE system. Therefore, it requires processing capabilities only for minimal computations and processing. The resulting platforms are compatible with use cases that manage messaging between authorized users. For healthcare, doctors and patients can use this platform to communicate within a secure network. As a result, the blockchain and E2EE system preserves the privacy between their conversations and keeps records immutable for better tracking and security. Another use case is for supply chain management. Suppliers and distributors can communicate about the status of deliveries and production in a tamper-proof space. Also, retailers and customers can discuss product details under a secure and private network.

B. Discussion of Advantages and Security Analysis

1) Data Storage Immutability: The private blockchain introduces immutability to the IM platform's data. With decentralization and cryptographic architecture, the blockchain ensures that data within it has high tamper resistance. Through its distributive nature, multiple copies of the blockchains across trusted servers allow cross-checking. As a result, it is easier to detect unwanted modification of data. Also, the cryptographically-linked blocks make it easier to catch any inconsistencies in messaging and account creation history. As a result, it guarantees data history accuracy and reliability.

2) End-to-End Privacy Protection: The E2EE created by incorporating public key encryption adds another layer of security to the platform. It ensures that data remains private even as it is within the blockchain. One of the vulnerabilities of blockchains is its transparency, as its data is easily accessible to all its trusted users. Introducing E2EE keeps that data only visible to relevant parties. All messages between two users are only accessible with the corresponding private key. And since only the message recipient can decrypt it, even the server does not know what information each user is sharing. As a result, it keeps user data private and provides better resistance against malicious attacks such as man-in-the-middle.

3) Web Service Decentralization: A REST API Web service further promotes the decentralized architecture we envisioned for our proposed platform. It regulates the blockchain by handling the indexing of its blocks and regulating its data entries through requests, providing a flexible means of accessing user information. Also, it contributes to the sustainability of the design as a well-established service for Web server interfacing. Its load-managing capabilities complement the blockchain's decentralized nature, creating a more distributive network that promotes proper process reallocation and load balancing.

A summary of these advantages, comparing them against centralized IM platforms and discussing other security benefits of our platform, is in Table II.

C. Future Works and Iterations

For future iteration of our work, we recognize that we only evaluated our design qualitatively against a general centralized IM platform. For future iterations of this letter, we plan to incorporate more experiments, such as latency and throughput, highlighting our design's feasibility through performance evaluations. We will strive to provide numerical evaluations of our platform that analyze the responsiveness and scalability of our design. Ideally, we aim to improve our proposed platform to cater to larger distributive systems.

V. Conclusion

We propose a secure IM platform using private blockchain technology, E2EE, and REST API Web interfacing to address data privacy and centralization issues of centralized implementations. We incorporated private blockchain technology to serve as the service's data storage. The E2EE implementation improves the platform's data privacy. Through public key encryption, E2EE preserves the privacy of user conversations. Implementing the REST API Web server provides a flexible means of handling blockchain data while catering to its decentralized nature through its load-balancing capabilities. Overall, through a proper deliberation of the advantages and security contributions of the proposed platform, we highlight its feasibility in addressing the data privacy and centralization issues of current IM services.

References

[1] T. Cai, Z. Hong, S. Liu, W. Chen, Z. Zheng, and Y. Yu, "SocialChain: Decoupling social data and applications to return your data ownership," *IEEE Trans. Services Comput.*, vol. 16, no. 1, pp. 600–614, Jan./Feb. 2023.

[2] X. Zhu, D. He, Z. Bao, M. Luo, and C. Peng, "An efficient decentralized identity management system based on range proof for social networks," *IEEE Open J. Comput. Soc.*, vol. 4, pp. 84–96, Mar. 2023.

[3] F. Li, X. Yu, R. Ge, Y. Wang, Y. Cui, and H. Zhou, "BCSE: Blockchain-based trusted service evaluation model over big data," *Big Data Min. Anal.*, vol. 5, no. 1, pp. 1–14, Mar. 2022.

[4] A. Theophilo, R. Giot, and A. Rocha, "Authorship attribution of social media messages," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 1, pp. 10–23, Feb. 2023.

[5] P. Piamjinda et al., "CHIVID: A rapid deployment of community and home isolation during COVID-19 Pandemics," *IEEE J. Transl. Eng. Health Med.*, vol. 12, pp. 390–400, 2024.

[6] S. Chakraborty, K. Mazumdar, D. De, and S. Kumar, "RMS: A delay sensitive road monitoring system using edge intelligence," *IEEE Sensors J.*, vol. 23, no. 3, pp. 2643–2650, Feb. 2023.

[7] A. Bozorgi et al., "I still know what you did last summer: Inferring sensitive user activities on messaging applications through traffic analysis," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 5, pp. 4135–4153, Sep./Oct. 2023.

[8] C. Gouert and N. G. Tsoutsos, "Dirty metadata: Understanding a threat to online privacy," *IEEE Security Privacy*, vol. 20, no. 6, pp. 27–34, Nov./Dec. 2022.

[9] H. Yi, "Secure social Internet of Things based on post-quantum blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 950–957, May/Jun. 2022.

[10] I. Vakilinia, W. Wang, and J. Xin, "An incentive-compatible mechanism for decentralized storage network," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, pp. 2294–2306, Jul./Aug. 2023.

[11] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A survey on blockchain for healthcare: Challenges, benefits, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 386–424, 1st Quart., 2023.

[12] X. Li and W. Wu, "Recent advances of blockchain and its applications," *J. Soc. Comput.*, vol. 3, no. 4, pp. 363–394, Dec. 2022.

[13] R. Du, C. Ma, and M. Li, "Privacy-preserving searchable encryption scheme based on public and private Blockchains," *Tsinghua Sci. Technol.*, vol. 28, no. 1, pp. 13–26, Feb. 2023.