2025 7th International Conference on Blockchain Computing and Applications (BCCA) | 979-8-3315-0296-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/BCCA66705.2025.11229731

CRUD-Chain: A Brownie Based Medical Records Management System

1st Mugdha Srivastava
Dundalk Institute of Technology
Dundalk, Ireland
mugdha.srivastava@dkit.ie

2nd Abhishek Kaushik
Dundalk Institute of Technology
Dundalk, Ireland
abhsihek.kaushik@dkit.ie

3rd Róisín Loughran
Dundalk Institute of Technology
Dundalk, Ireland
roisin.loughran@dkit.ie

***Abstract*—This demonstration introduces a Proof-of-Concept distributed application that establishes the use of blockchain for patient data management in a decentralised and secured environment. This work originates from the requirement of a secure and immutable system to store records while making sure that it has the ease of use of a Relational Database Management System. The primary goal of this work is to show how simple database operations - Create, Read, Update, and Delete - work in a blockchain environment. Since blockchains are usually append only, we present a system that gives a patient the right to be forgotten if they want it by introducing a deletion flag that marks the data so that it becomes inaccessible to everyone including the database admin. This system has been created using the Ethereum Brownie environment because it enables rapid prototyping in python.**

***Index Terms*—Blockchain, Healthcare, Patient Data Management System, Decentralisation**

I. Introduction

Human data is among the most valuable resources of the digital age, making the consequences of regular data breaches increasingly profound and debilitating [1]. A primary way to target human data, such as that generated in hospitals, is by attacking centralised relational Database Management System (RDBMS) that can disrupt treatment processes, delay progress, and potentially endanger patient lives [2] [3].

While centrally managed RDBMS remain prevalent in hospitals primarily due to ease of use, blockchain offers secure and transparent sharing of medical records between different healthcare providers while maintaining patient privacy through permissioned blockchain networks [4]. However, blockchain's immutability presents challenges with GDPR's "right to erasure" requirements, as data cannot be easily deleted or modified [5].

To address this, the CRUD-Chain blockchain setup allows the user to Create, Retrieve, Update, and Delete (CRUD) records like an RDBMS which is still the preferred data storage method for healthcare organisations. Thus, this work presents a blockchain that has the operational flexibility of an RDBMS while having the security and availability of a distributed system. We selected Ethereum's Brownie development environment due to its robust support for blockchain development in python on the Ethereum network, offering a streamlined and efficient framework for implementing and testing smart contracts.

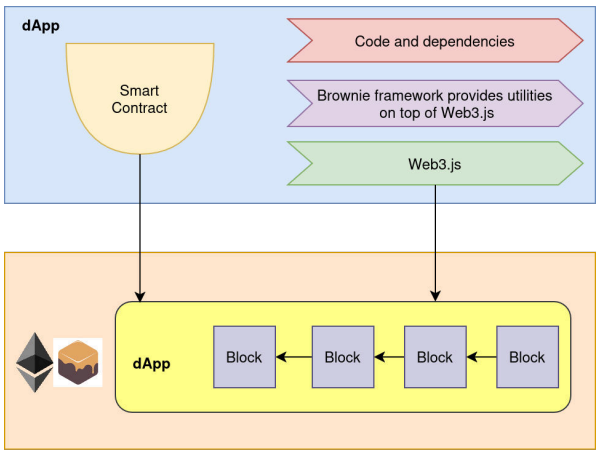

Fig. 1. Architecture diagram of CRUD-Chain

II. System Design and Architecture

In this work, we propose a blockchain-based system to manage patient data, designed to ensure secure, immutable, and decentralised data handling. The system configuration utilises a robust network setup that includes Ganache CLI integrated with MetaMask to simulate a blockchain environment (see Figure 1). The framework used for testing, deployment, and debugging is Brownie. For backend integration, Node.js has been implemented to facilitate seamless user interaction with the blockchain, and Web3.js is the library used for interacting with the Ethereum blockchain ensuring a smooth and responsive connection between the application and the decentralised network. The architecture of the system consists of key components, such as a smart contract written in Solidity to govern the rules of data access, storage, and sharing (see Figure 2). The data in this system is stored on-chain for faster processing time. Solidity mappings do not support directly removing entries but this code makes sure that the chain remains intact by including mechanisms like a soft deletion flag (isDeleted) and validation to prevent duplicate IDs. This approach also avoids potential issues with re-indexing or reusing mapping keys, ensuring a smoother and more reliable handling

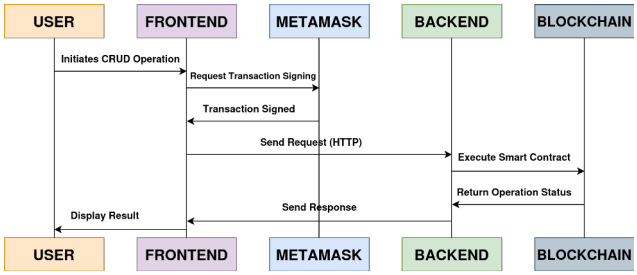

Fig. 2. Sequence diagram of CRUD-Chain

of data while making sure that the removed data stays inaccessible for everyone including the admins and creators of the system.

III. Demonstration

The system was tested on the Ganache-CLI through its front-end (see Figure 3). For user visibility, the blockchain was also added to the frontend but with minimal details containing the block hash, the block timestamp, the transaction count and the transaction hash only. The Ethereum gas limit for transactions is set at 6,721,975. The results demonstrated that transaction costs varied based on the operation performed. Deploying the smart contract consumed a significant portion of this limit, utilizing 738,838 gas (10.99% of the entire limit). For subsequent operations, the average gas used, over 10 inputs, for inserting a new record onto the blockchain was 107,909.1. Updating an existing record, specifically changing only the name while retaining the disease information, required an average of 37,098 gas. Deleting a record, which was implemented as a soft deletion by setting an isDeleted flag to true, consumed 45,943 gas for all records regardless of the record's size. In terms of latency, data retrieval operations showed no observable delay and no gas was used for querying, indicating efficient access times within the system.

IV. Future Work

Future work will address key limitations by advancing GDPR compliance, particularly the "right to be forgotten," through advanced data erasure methods. Sensitive health data will be stored off-chain using encrypted solutions such as InterPlanetary File System (IPFS), with blockchain integrity maintained via hashed pointers. Enhanced cryptographic measures and robust user management, including Role-Based Access Control, authentication, and authorisation, will safeguard confidentiality and restrict access. The system will also be aligned with healthcare data standards, and a user-friendly interface will be developed to encourage adoption.

In addition, scalability and economic feasibility will be evaluated by simulating large-scale, realistic deployments and analysing gas and storage costs. Layer-2 solutions such as Polygon will be considered to

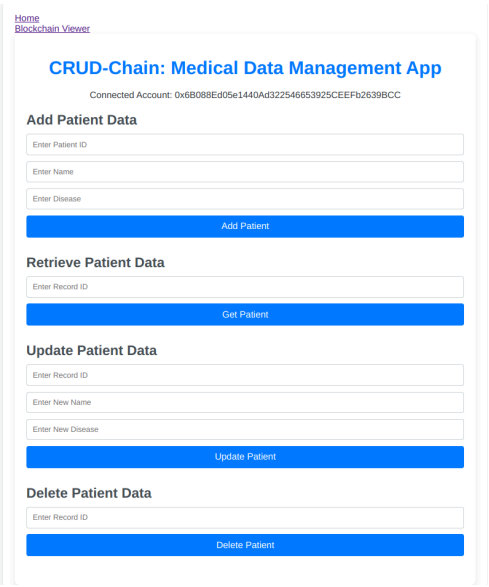

Fig. 3. View of the home page of the dApp.

reduce fees and improve performance, while off-chain storage will help manage data growth. Security will be reinforced through comprehensive threat modelling and high-load testing. Finally, benchmarking against existing blockchain CRUD systems will be done to support the system's unique contributions and practical advantages.

Acknowledgment

This publication has emanated from research conducted with the financial support of Research Ireland under Grant number 21/FFP-A/9255.

References

[1] Gabriel Arquelau Pimenta Rodrigues, André Luiz Marques Serrano, Amanda Nunes Lopes Espiñeira Lemos, Edna Dias Canedo, Fábio Lúcio Lopes de Mendonça, Robson de Oliveira Albuquerque, Ana Lucila Sandoval Orozco, and Luis Javier García Villalba. Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, 9(2):27, 2024.

[2] Karuna S Bhosale, Maria Nenova, and Georgi Iliev. A study of cyber attacks: In the healthcare sector. In *2021 Sixth Junior Conference on Lighting (Lighting)*, pages 1–6. IEEE, 2021.

[3] Mugdha Srivastava, Abhishek Kaushik, Róisín Loughran, and Kevin McDaid. Data poisoning attacks in the training phase of machine learning models: A review. *32nd Irish Conference on Artificial Intelligence and Cognitive Science*, 2024.

[4] Farida Habib Semantha, Sami Azam, Bharanidharan Shanmugam, and Kheng Cher Yeo. Pbdinehr: A novel privacy by design developed framework using distributed data storage and sharing for secure and scalable electronic health records management. *Journal of Sensor and Actuator Networks*, 12(2):36, 2023.

[5] Marina Valpītere. "right to erasure" and private blockchain in the european union: legal requirements and technical possibilites. 2020.