Blockchain Database - Project Summary

Julia Kulczycka, Viktoria Kashpruk, Miłosz Krzysiek, Maciej Szałasz

Project Overview

The main objective of this project was to explore blockchain as a means of implementing a secure and efficient data storage system. Our solution focuses on a system for medical institutions, enabling doctors to store and manage patient data with enhanced privacy and security. The use of blockchain ensures that sensitive information is protected while maintaining integrity and traceability.

What Was Accomplished

Transaction Signing and Verification

Every transaction uses a doctor's private key, transaction ID, and content to generate a unique signature. This allows transaction data to be verified using the doctor's public key. Each transaction must be confirmed to ensure that no fake or harmful data is inserted into the database.

Calculation and Verification of Proof-of-Work (PoW) System

Every block in the blockchain includes PoW (Proof of Work). PoW is a value that, combined with the block's data, allows for the calculation of a hash with a specified number of leading zeros. This is a computation-intensive task that introduces a delay in block creation and provides an additional layer of verification.

Simplified Blockchain Structure

Our blockchain system has a single main branch where all blocks are added sequentially.

Local Medical Institution Network Simulation and Interaction

All medical institutions emit their transactions to the network. After a time delay, the emitted transactions are verified and included in a newly created block.

Command Line Interface (CLI)

The database can be accessed through a command-line interface.
There is an option to log in or sign up to the system and depending on the role (doctor or patient) emit the transaction or read the transaction for the patient.

Patient Data Encryption

The system supports encryption of sensitive patient data to enhance security. The doctor creates transactions which are encrypted and can be read by both doctor and the patient using their respective private keys.
This ensures that in case of any database leaks the user data remains safe.

What Was Not Accomplished

True Blockchain Structure

Our database does not implement a truly decentralized blockchain structure. It simulates the concept but still relies on centralized network management.

True implementation was not achieved due to:

- **Lack of initial knowledge about blockchain:** A true implementation would have required a significant project restructure, including changes to most of the existing architecture.
- **Time constraints:** The goal could have been achieved with a longer time frame and greater focus on its implementation.

This objective could serve as the main goal for further development of the project.

Key Project Takeaways

Blockchain

Implementing a simplified blockchain allowed us to understand the differences between our implementation and real-world blockchain systems. We gained insight into the guidelines blockchain imposes and the mechanisms behind its trust system.

Cryptography Behind Blockchain

We successfully implemented cryptographic techniques that enable blockchain to securely execute and store transactions, including transaction signing, verification, and PoW calculation.

Code Quality

The project's code is clear and well-structured. We became familiar with code quality checkers and formatters such as MyPy, Black, Isort, Pre-commit, and others. These tools helped us maintain high coding standards.

Teamwork

We learned the importance of good project organization and effective task delegation, which were key to our success.

Summary

We are satisfied with our work. The project turned out to be demanding in terms of research, but this challenge pushed us to be more determined in its implementation. We gained a great deal of knowledge about blockchain, code quality, and effective collaboration. Even the unmet goal contributed to a deeper understanding of the subject and the complexity of real-world systems based on blockchain.