De La Salle University - Dasmariñas

MEDICHAIN

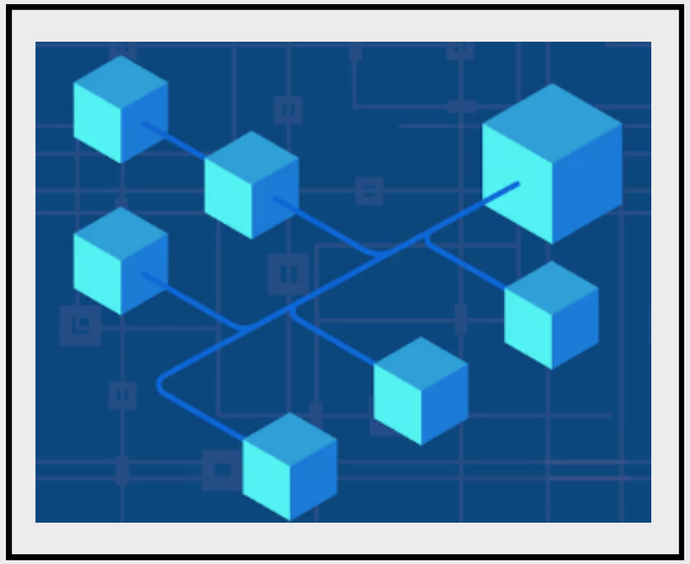
Blockchain-Based Patient Data Repository with Homomorphic Encryption for Secure Decentralized Healthcare Queries

Presented by:

Batino, John Rafael C. | Paulan, Renz Aaron C. | Quitaneg, Blake Daniel M.

First of all...

WHAT IS BLOCKCHAIN?



Blockchain is a decentralized, distributed ledger technology wherein it securely records transactions across multiple nodes. Each “block” in the chain contains a collection of records, a timestamp, and a hashed link to the previous block, creating a secure and chronological chain of data.

Features:

- Decentralization - eliminates single points of failure
- Transparency - all certified users can view and verify the stored data
- Immutability - no consensus = no data alterations
- Security - hashed “block” links

INTRODUCTION

Background:

- The growing need for secure and efficient healthcare data management.
- Blockchain's potential in enhancing transparency, security, and integrity.
- Introduction of MediChain – a system that employs blockchain and homomorphic encryption to secure patient data.

Research Questions:

- How can blockchain improve security, data integrity, and privacy for medical repositories?
- What challenges arise when using blockchain for decentralized medical data management?

STATEMENT OF THE PROBLEMS

ISSUES WITH TRADITIONAL SYSTEM

- Centralized storage vulnerable to data breaches and unauthorized access.
- Lack of patient control over personal health records.
- Inefficient and insecure data processing.

CHALLENGES WITH BLOCKCHAIN ADOPTION

- Complexity, scalability, and cost of implementation.
- Integration issues with existing legacy healthcare systems.
- Privacy concerns related to encrypted data processing.

OBJECTIVES

01 Design a private blockchain and implement smart contracts, Proof of Authority consensus algorithm, and homomorphic encryption

02 Create APIs to enable secure communication between the blockchain backend, frontend application. and the database system

03 Test the blockchain system to verify the functionality, security, and reliability of the system

04 Address identified challenges and optimize the system's performance and security

METHODOLOGY

Research Design:

- Descriptive-Developmental Approach: Build and assess the MediChain system.
- Emphasis on developing, testing, and validating the blockchain system.

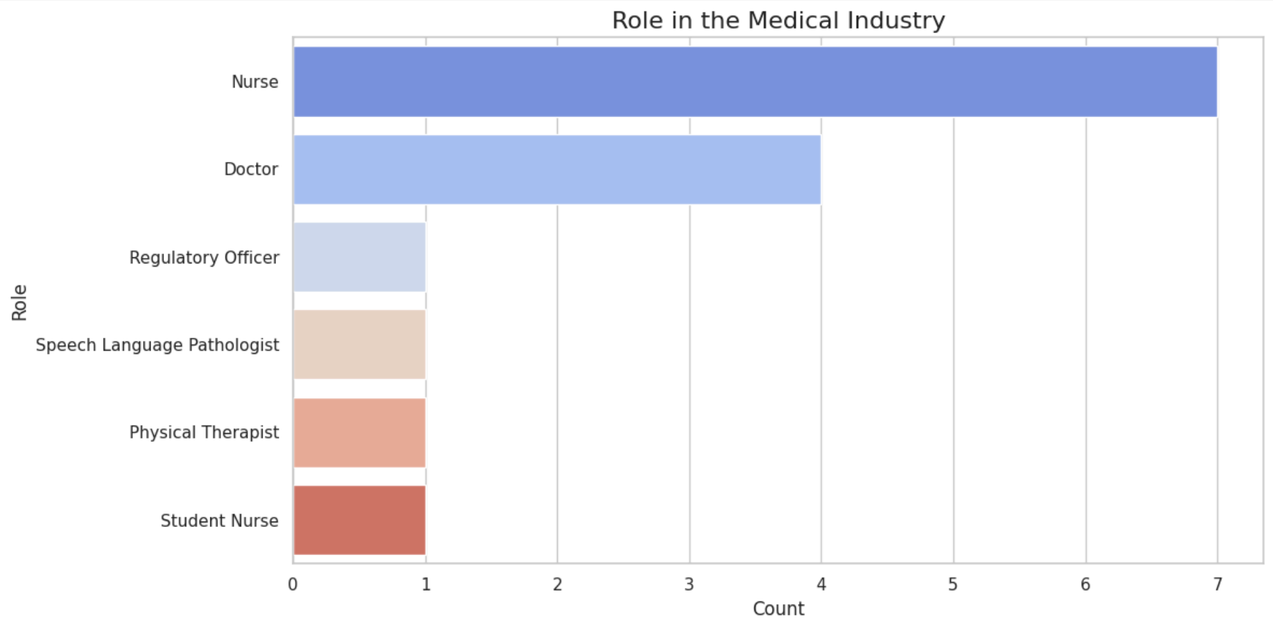
Tools and Techniques:

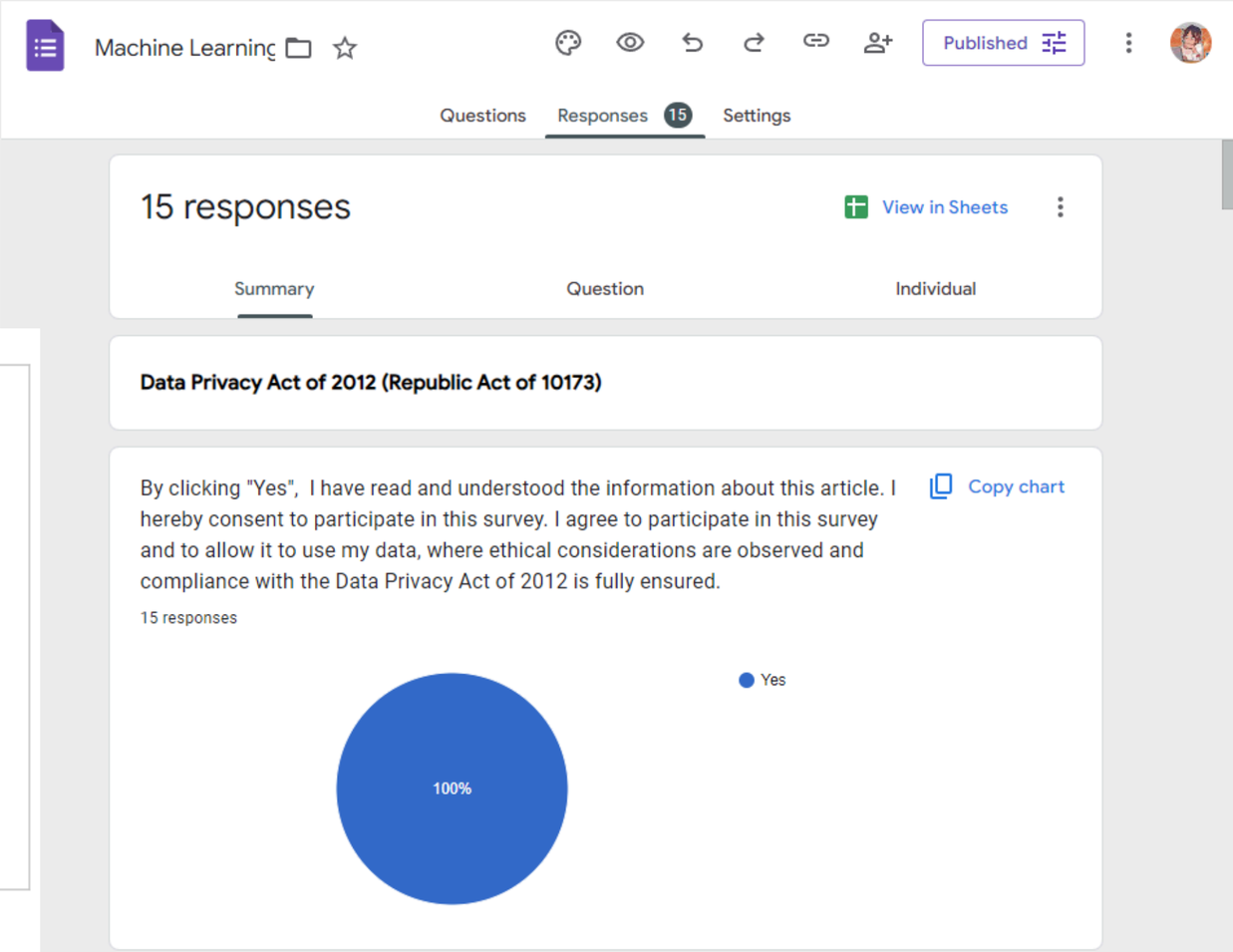
- Programming Languages: Python for backend logic, HTML/CSS/JS for UI.
- Data: Mock patient datasets from Kaggle used to simulate patient records.
- Encryption: Homomorphic encryption to ensure security and privacy.
- Consensus Mechanism: RAFT algorithm for reliability and performance.
- APIs: Enable communication between blockchain backend, frontend, and database.

METHODOLOGY

Participants:

- Survey of medical professionals with experience in managing patient records.



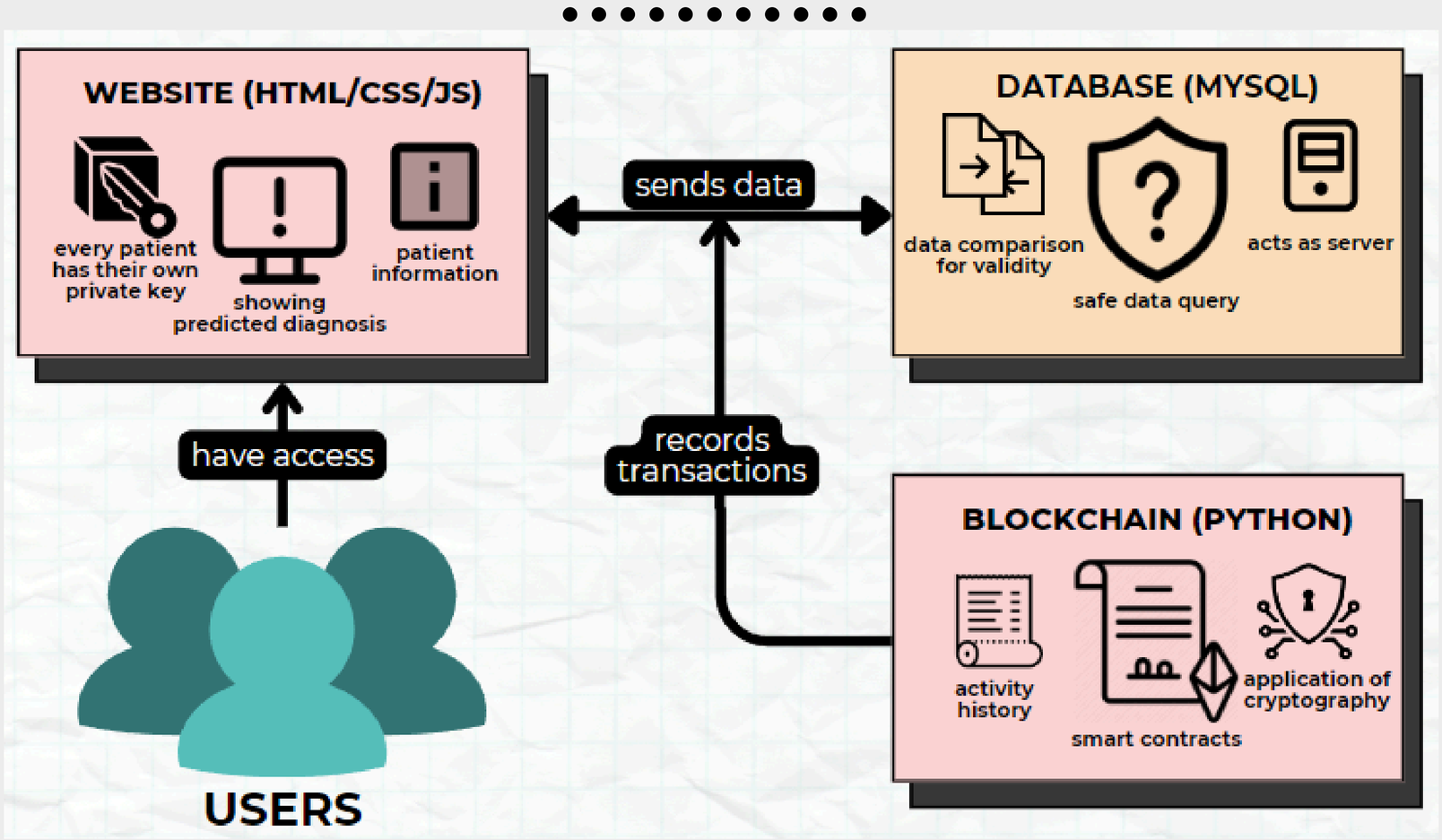


SYSTEM DESIGN AND ARCHITECTURE

SYSTEM COMPONENTS

- Private Blockchain: For secure and controlled access to patient data.
- Nodes and Consensus: Proof of Authority algorithm for data consistency.
- Chaincode (Smart Contracts): Automate transactions on the blockchain.
- APIs: Enable communication between different components of the system.
- Encryption Layer: Homomorphic encryption for secure processing of encrypted data.

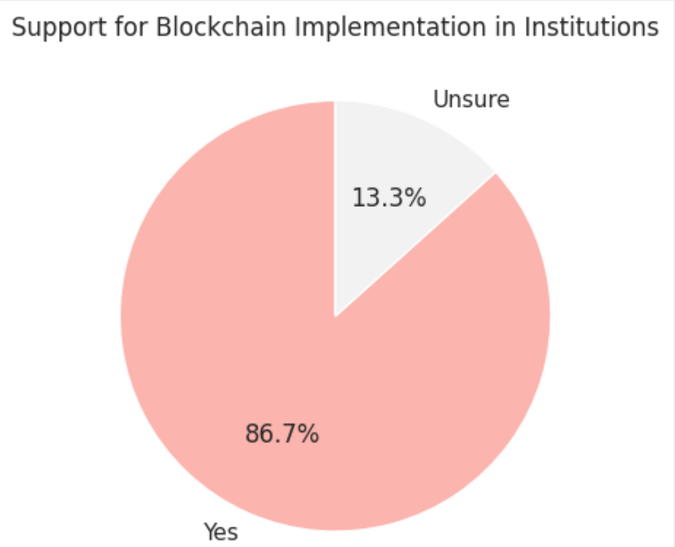
DATA FLOW

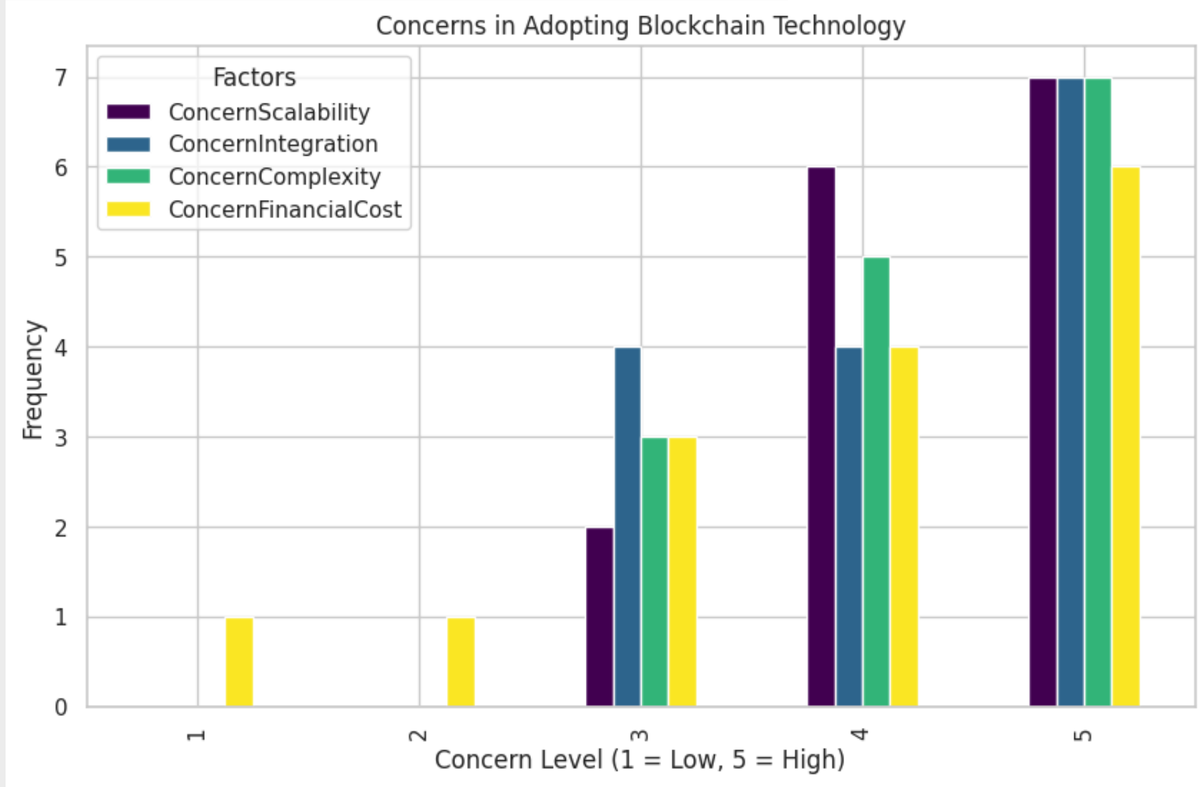

WEBSITE (HTML/CSS/JS)
every patient has their own private key
showing predicted diagnosis
patient information
sends data
DATABASE (MYSQL)
data comparison for validity
safe data query
acts as server
have access
records transactions
USERS
BLOCKCHAIN (PYTHON)
activity history
smart contracts
application of cryptography

RESULTS AND ANALYSIS

SURVEY RESULTS FROM MEDICAL PROFESSIONALS

- Awareness of blockchain: Most were unfamiliar with blockchain, but many were willing to adopt it.
- Key concerns: Scalability, system complexity, cost, and privacy issues.
- Adoption willingness: 86.7% of respondents are willing to adopt blockchain systems in their medical institutions.





RESULTS AND ANALYSIS

SYSTEM TESTING RESULTS

- System Performance: Evaluation of transaction speed and blockchain efficiency.
- Homomorphic Encryption: Computational performance impacted slightly, but security was maintained.
- Proof of Authority: Ensured consistency and reliability in the blockchain system.
- Security Improvements: Enhanced protection from single points of failure and unauthorized access.

DISCUSSION

Impact on Healthcare:

- Data Integrity: Immutability and integrity of patient records are guaranteed.
- Fraud Prevention: Reduction of fraudulent medical claims and errors.

Technical Challenges:

- Homomorphic encryption causes performance bottlenecks.
- Integration with existing medical systems is difficult due to legacy infrastructure.

Regulatory Challenges:

- Compliance with the Data Privacy Act (Philippines) and GDPR (EU) is required.

CONCLUSION

- MediChain demonstrates how blockchain can be used for secure healthcare data management.
- The system improves data security, integrity, transparency, and patient control.
- Use of homomorphic encryption ensures data privacy during processing.
- RAFT consensus mechanism provides efficient consensus with low computational overhead.

Call to Action:

- Encourage healthcare institutions to explore blockchain for patient data management.
- Call for further development to address scalability, privacy, and cost challenges.

THANK YOU

Presented by:

Batino, John Rafael C. | Paulan, Renz Aaron C. | Quitaneg, Blake Daniel M.