Health Ledger using Blockchain

Why use Blockchain?

- Health ledger implemented using blockchain would prove to be an innovative answer to the demand for decentralized and secure storage of the health history with simultaneous personal access control.
- Emergent trends around the use of Blockchain, or Distributed Ledger Technology, offer solutions to some of the problems faced in enabling these technologies, especially to support consent, data exchange issues.

Problems in conventional health databases

- Conventional database systems are managed by powerful stakeholders and institutions, having power and reason to force their hand.
- Databases support data manipulation operations like create, read, update, and delete, which compromises privacy and security.
- With conventional health databases there always exists the risk of single point of failure.

How does blockchain fit in?

- Decentralized management: Blockchain is a peer-to-peer, decentralized database management system.
- Immutable: Blockchain only supports create and read functions i.e, it is very difficult to meddle with the data or records.
- Secure: Blockchain improves security and privacy using asymmetric cryptography.

About the Project

User can access the following functions using the ledger:

- Create a block
- View personal details
- Edit personal details
- View other user’s details

Encryption

We use Asymmetric Key encryption.

Users are provided with two keys

1. Private key: A nonce value is generated in the form of a number. This number is used to view or update one’s medical records.
2. Public Key: This key can be used to access other users data. This is encrypted name of the user.

Methods implemented

- createBlock():

  Takes input from user. Then encrypts the user's name into a hash to create the public key. Then data string is mined and the block is added to the chain.

- verify_transaction() :

  Receives inputs from verifier and prover to implement the zero knowledge proof. Computes and verifies if the values at both end match. Returns the result as true or false.

Methods implemented

- mineBlock():

  Takes user data string as input and mines the block. A simple puzzle is chosen to create proof of work. The obtained nonce value is then displayed.

- viewOtherUser():

  Given the encrypted name of the user, our name be present in their permitted users list, it displays the data of the user. Utilizes zero knowledge proof by calling verify_transaction().

Improvements that can be made

- Currently the information that is present in the blockchain is dynamic, that is, the information is present only as long as the program is running. The usage of a database can help in permanent storage of information.

- The ledger can turn into an interactive user platform with the build of GUI.

Conclusion

In the current scope the health ledger demonstrates the various steps involved in implementing blockchain based systems.

The health ledger puts to display key blockchain features like immutability, peer-based distribution and enhanced security features.

All in all the project has immensely helped in building an understanding of blockchain development process.

Team members

- B S R Nanda Kishore - 2016AAPS0238H
- Vikranth Korata - 2016AAPS0229H
- Valluri Manoj Kumar - 2017A7PS0040H
- Harshavardhan Bodepudi - 2017A4PS0546H
- Vishnu Vardhan M - 2018A7PS0482H