Survey on Identity Management using Blockchain Technology

Mardavkumar Gandhi
Computer Science & California State University, Sacramento,
United States

Abstract— In the present interconnected world, digital IDs are used to demonstrate identity. These IDs prove to be only tangentially related to the service being accessed and requires us to apply a significant amount of privacy. The current systems possess number of problems such as proxies but blockchain proves to be the solution for this type of Identity related problem.

Markers of identity are often required to be very personal pieces of data. Consider a list of personal information collected when someone opens a savings account, such as address and identification (driver’s license or passport). It’s easy to take these pieces of data for granted, as we’ve generally become accustomed to handing them over at the drop of a hat. But let’s take a moment to consider what giving up these pieces of identity really means and whether is it necessary?

In handing over a passport to a banker, a person gives the bank full permission to record not only their date and place of birth, but also everywhere he or she has toured.

In order to solve above privacy problem and to make Identity sharing process more user friendly I have implemented an Identity Management System with Blockchain technology with the help of hyperledger fabric framework.

Keywords— Blockchain, hyperledger, transaction, identity, network

I. INTRODUCTION

A blockchain is basically a shared digital ledger which helps in recording all the transactions in some public or private network. All the members that are there in the network are connected and any kind of transactions are recorded in the ledger are permanently recorded. This is stored in the sequential chain of the cryptographic hash blocks that records the history of all the different kinds of transactions. The transactions that are committed and validated are linked to the most recent transaction in the form of chain hence clearly justify the name i.e. blockchain. Therefore, one can say that blockchain act as the single source of truth. With the block-chaining the network will look as shown in the below figure[1].
There are many different benefits of using block-chaining some of them are discussed as follows:

- By using blockchain shared ledger different organizations can save time and cost.
- It provides consistent dataset with least errors and flexibility to the users in a way that they can edit the dataset they own and the changes will be reflected in the ledger.
- This mechanism has gathered trust of the users as the source of information cannot be owned by any participating member or node in the network. Hence, it inculcates the integrity and trust in the information flow in the participating nodes.
- Since different transactions are automated, smart and final hence, the business organizations can benefit from the speed of execution, reduced cost, reduced risk.

**Hyperledger** is an open source blockchains. It is a platform for distributed ledger solutions underpinned by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability. The objective of this is to advance cross-industry collaboration by developing blockchains and distributed ledgers, with a particular focus on improving the performance and reliability of the systems. It is basically used to deliver scalability, confidentiality and flexibility.

Hyperledger Fabric is one of the blockchain projects within Hyperledger. Like other blockchain technologies, it has a ledger that uses smart contracts, and is a system by which participants manage their transactions. It differentiates from some other blockchain systems is that it is private and permissioned. Rather than an open permission less system that allows unknown identities to participate in the network (requiring protocols like Proof of Work to validate transactions and secure the network), the members of a Hyperledger Fabric network enrol through a Membership Service Provider (MSP).

It has a ledger subsystem comprising two components: the world state and the transaction log. Each participant has a copy of the ledger to every Hyperledger Fabric network they belong to.

The world state component describes the state of the ledger at a given point in time. It’s the database of the ledger. The transaction log component records all transactions which have resulted in the current value of the world state. It’s the update history for the world state. The ledger, then, is a combination of the world state database and the transaction log history.

The ledger has a replaceable data store for the world state. By default, this is a Level DB key-value store database. The transaction log does not need to be pluggable. It simply records the before and after values of the ledger database being used by the blockchain network figure[1].

**II. ARCHITECTURE OF IDENTITY MANAGEMENT SYSTEM**

![Hyperledger-fabric model](image)

Figure-2
The Basic working of Identity Management using blockchain technology is as follows:

- Whenever the user uploads the document, this is a transaction and all details of transaction collected in a block.
- A block is then broadcasted to all the parties (i.e. all the system in network which is holding the data) or we can say to all the network peer (as shown in Figure-2).
- All the network peers will validate the transaction and the block will be added to chain and user will successfully upload the document in his account.
- As shown in below figure-4 each will successful transaction will have Blockchain Transaction ID and Document ID whenever the document is uploaded, and the document will have document signature also which ensures that unauthorized person cannot modify the document and it provides authenticity of the valid document and transaction.
- After successful transaction, this transaction will be recorded on public ledger (as show in Figure-2) which will be visible across the network.
- Whenever Department will request access for any particular document of user, this will also be one new transaction and as discussed above, this new transaction will also be stored on block and block will be broadcasted to all the network peers and after approval of all network peers this block will added to the new transaction.
- After the block is added to the new transaction, intended user will be able to see the document request in his access request tab.
- When user will approve or reject the request this information will be stored in new block and the new block will be broadcasted to all network peer and after approval of all the network peers this block will be added to the same blockchain transaction which was started by the department by requesting to that document.
- When this second block will be added to that blockchain, it will be having hash of previous block also, so if anybody wants to change the specific block in the block of chains they have to correctly recompute the hash value of all the blocks in the chain which is computationally impossible, and this makes the transaction secure.
- In order to depict the Identity Management System using blockchain technology, I created hyperledger fabric network which will be having 2 network peer which will be holding the data using level DB and front end and backend will be tied up using docker (shown in Figure-3)
- There are basically two entities
  - Department
  - User
- User will register and store the different documents in different drawers based on the type of document.
- Department can search for the user and can see what type of documents user is having and department can request to access the specific document.
- User will approve or reject the access request as per the need.
III. IMPLEMENTATION

1. In Ubuntu which is working as our docker We First Run the script (Bash script) which will start the hyperledger network server and after the Network is up, script will start the NodeJS server which is working as backend of our Identity Management Application. We will expose the Front End after Node server and network server is up.

2. As Soon as the Front End is up user/Department will perform the operations.
   Node server will be having scripts written in Go language which will invoke or query the data in Hyperledger peer based on post or get action from front end.

3. We are storing the transaction details, documents etc in Hyperledger Database (level DB - in-memory database)

4. Based on Key-Value pair we will fetch or store the data in In-memory Database (Level DB)

5. We have Used HTML, CSS, Java script for Front End and Go Language for Node Scripting for backend.

IV. SOLUTIONS PROPOSED AND RESULTS

The main security concern with current identity systems is that sensitive personal data is stored in vulnerable central repositories owned by third parties. The blockchain, on the other hand, moves control over data to the edges of a network and distributes it across multiple endpoints. With distributed data, attackers must hack each endpoint and overcome the layers of security associated with each, instead of gaining access to a single database.

In addition, identity solutions that leverage blockchain technology can eliminate user friction by putting individuals in control of which data they share with third parties. The proposed solution explains the concept of “personal cloud” that allows users to reveal individual pieces of information to different service providers as required, rather than handing over an entire bundle of personal information.

Technology built on the blockchain also allows for greater access by those who cannot (or choose not to) conform to current standards of verification. Rather than relying on third-party forms of identification, such as government-issued passports or ID cards, this vision of the future allows services (such as bank accounts and remittances) to be accessed by validating one’s identity on the blockchain.

The proposed solution uses hyperledger fabric which is a blockchain framework implementation which is intended as a foundation in developing applications. It also allows components such as consensus, Member Services. It uses smart contracts called “chain code” which comprises the application logic of the system. The smart contract is written in Go language and the hyperledger network will be setup on ubuntu with 2 peers and a member service. The underlying client application will be built using bootstrap HTML5, CSS and JS deployed on a server.

V. CONCLUSION AND FUTURE ENHANCEMENT

Future Enhancement
A few recommendations for improvement are as follows:

- Instead of In-memory Database (Level DB) we can implement/migrate the system to Relational Database like MySQL or Oracle.
- Instead of just limiting this application to document sharing, we can apply this blockchain technology and can build system which will allow user to have just single digital ID for all access.

Conclusion
Identity Management System which is built using blockchain technology solve the problems persisting with existing Identity Management system and it provides more secure, Immutable and user convenient system.
REFERENCES


