Blockchain based Asset Registration & Management System

Vedant Tilavankar[1], Abhishek Yadav[2], Sai Pisey[3], Vaishali Yeole[4]

[1,2,3,4]*Dept. of Computer Engineering ,Smt. Indira Gandhi College of Engineering , Navi Mumbai, Maharashtra, India*

---***---

Abstract—Since the beginning of Bitcoin in January 2009 by Satoshi Nakamoto, the thought of creating products & solving existing real-life problems in all facets of life with non-centralized technology i.e This has created a large number of possible use case possibilities. A huge amount of potential applications - right from education to healthcare to defense have been theorized and many have been implemented. With the emergence of the feature-packed, extraordinary Blockchains like Ethereum & frameworks like Hyperledger Fabric, the process of developing Blockchain-based software and products has been expedited & simplified. This paper states about the various applications of Blockchain - 'Asset Registration & Management' and discusses various concepts, fundamentals & ideas attributed to the same.

Keywords— ***Hyperledger fabric, Smart contracts, Blockchain, Assets.***

I. INTRODUCTION

Generally, in centralized systems data is stored sequestered, in one place, which makes it vulnerable to attacks and also hampers availability in case of system failures. Although contemporary data storage solutions offer ways and workarounds for these problems, issues like data leaks, tampering of data, introduction of fraudulent data by malicious actors are common. With global digitization, innovations in technology and increase in the instances of cyber attacks, the trust factor of centralized systems has taken a hit.

In such situations, the features of Blockchain Technology can be leveraged to create safe systems which become safer the more populated they get - an example of such implementations being Bitcoin. However, if we talk about storing assets on Blockchain, we need some control over who can upload assets, who can download assets and something that dictates what the entire process should be. This is a use case of Smart Contracts and permissioned Blockchains like Hyperledger Fabric. Through this project, we attempt to create a system where a specific set of people - like the employees of an organization or the members of a trust, can store and transact their assets via blockchain - they can upload, download, transfer, update, delete assets, provided they have the required permissions.

II. LITERATURE SURVEY

The need for blockchain-based identity management is especially obvious in the internet age, according to a paper [1] by Ori Jacobovitz. We have encountered identity management difficulties since the beginning of the Internet. Security, privacy, and usability are three of the most important of them.

Permissioned blockchain as mentioned in an article of 2021 [2] - To become a node on a Permissioned blockchains, one would need authorization from one or several parties. The Sovrin Blockchain is an instance of a Permissioned Blockchain. Sovrin is administered by a group of nodes known as Stewards. This is done to ensure the validity of the data written on the ledger, which in this case is related to digital identification. The Sovrin Foundation trusts and vets its stewards. We're using IBM's Hyper Ledger Fabric network, which is similar to Sovrin's blockchain technology.

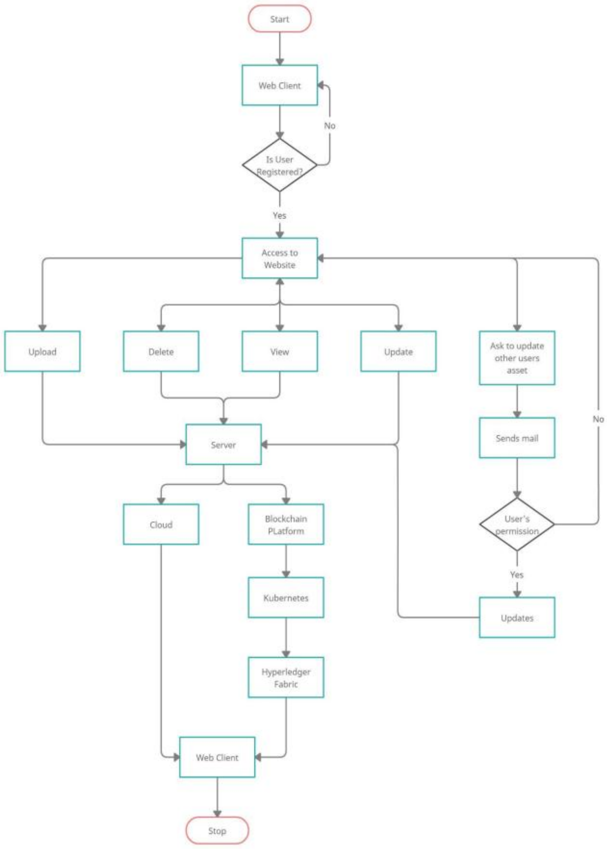
Suporn Pongnumkul, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong[3] investigated the performance of Ethereum and Hyperledger Fabric as private blockchain platforms with varying transaction volumes. When workloads of up to 10,000 transactions were involved, they determined that Hyperledger Fabric gave faster throughput and lower latency than Ethereum. Hyperledger Fabric's average throughput fluctuates at a far faster rate than Ethereum's. On the other hand, Ethereum can execute more transactions at the same time while using the same processing resources. In the future, Hyperledger Fabric will be able to support a huge number of concurrent transactions with the same computational resources.

The University of Bologna's Luca Foschini, Andrea Gavagna, Giuseppe Martuscelli, and Rebecca Montanari [4] analyse the Fabric platform's transaction performance by pinpointing the pieces that contribute the most to total overhead at a fine-grained degree level. They were particularly interested in how the programming language used to generate the chaincode as well as the number of participating endorser peers influence transaction delay. They were particularly interested in how the programming language used to generate the chaincode as well as the number of participating endorser peers influence transaction delay.

METHODOLOGY

Transacting and interchanging assets is a crucial part of human development. A digital asset is anything that can be saved and transmitted digitally (using a computer) that can be owned and thus, can have ownership and usage rights associated with it. Due to the adversity and uniqueness of digital assets, ranging from audio files to video files, pdfs, docs to any type of documents, the scope of our project only extends to digital assets that can be tokenized using a cryptographic protocol, or so-called crypto assets.

Digital Asset Management Systems(DAMS) ensure that operations or actions are only performed on a digital asset by individuals or organizations or any department that have the right access to the rights and permissions for the asset.



III. METHODS

So in any Digital Asset Management system, there can be a lot of users and these users can have the ability to perform various actions on the asset in the system based on the authority they have. Following actions user can perform regarding the asset and website are as follows:

1)User registration and user login

2)Viewing all the assets in the system

3)Viewing assets owned by the user currently logged in

4)Uploading a new asset

5) Deleting a new asset

6)Suggesting edits to an existing asset.

7) Viewing suggested edits for an asset that is owned by the user that is currently logged in.

8)Approving or denying suggested edits for an asset that is owned by the user that is currently logged in.

9)Allowing other users the permission to update an asset owned by the user that is currently logged in.

10)Assigning another user as an owner of an asset that is owned by the user that is currently logged in.

11) Downloading an asset.

III.I User Registration and User Login

For User Registration and Login System we have used utmost security standards. Passwords that users are going to use for registrations or for login purposes would be secured through a rigorous hashing process and would be hashed by bcrypt hash to make the identity of an user very secure. Login information would be stored in cookies on the browser, so that the site can recognise the users and their activities can be monitored.

III.II Uploading an asset

Users have to login before uploading an asset. Once an asset is uploaded, that asset would be sent to the node server and that node server would in turn send the asset to the cloud platform. From that cloud platform it would go to IBM blockchain platform from which a block would be instantiated and that asset would be distributed in the network using smart contracts.

III.III Viewing all existing assets in the system

In a blockchain system, since every block is connected to each other. Whenever a new asset is uploaded it must be verified by every node in the network since every node in the network has a complete copy of the blockchain. Therefore once an asset is uploaded it is visible to all the users in the network.

III.IV Suggesting edits, Viewing edits, approving or denying those edits.

In a blockchain network where a complete copy of blockchain is available to all the nodes, therefore everyone on the network can see the asset uploaded by any other user. So if some user wants to suggest some edits then that can be done. Viewing of those suggested edits is also possible, but since the person who suggested the edits has no right over the asset, that user cannot edit that asset. Therefore the owner has to approve or deny the request made by the other user.

III.V Allowing other user to edit an asset, Assigning other user as the owner of the asset

In our blockchain project if the user wishes to allow other users to edit some contents of the asset, then the owner of the asset can give permission to the user who wants to edit. The owner of the asset can also assign other users the ownership of the asset. This feature proves to be quite important in certain use cases of an organization or in NFTs or to provide licensing to other users etc.

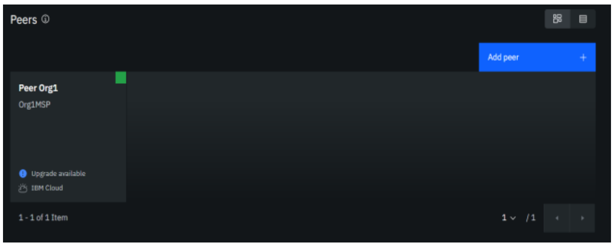
III.VI Modules and functions of the system

In this system we have first packaged smart contracts using IBM blockchain platform. Next, we have created a Hyperledger Fabric Network on IBM blockchain platform where smart contracts are installed and instantiated.Then we have set up an IBM cloud storage instance in order to retain digital assets uploaded to Digital asset management application. Next, we have set up an SMTP server on mailtrap to test email notifications sent by the user. Finally we have created a Vue.js web application, which makes use of the Hyperledger Fabric SDK, to be used to interact with the network.

III.VI.I Peer system

At a conceptual level, a blockchain network is composed mainly of organizations (as organizations decide on how a network is structured, as well as owning nodes and managing identities). At a physical level, however, a Hyperledger Fabric blockchain network is consisted of primarily of peer nodes that are owned and organized by organizations. Nodes are the fundamental elements of the blockchain network because they host ledgers(database) and smart contracts (which are contained in chaincode), and are therefore where transactions are performed and authenticated.

More accurately, the peer hosts instances of the ledger, and instances of smart contracts. Because smart contracts and ledgers are used to encapsulate the shared processes and shared information in a network.

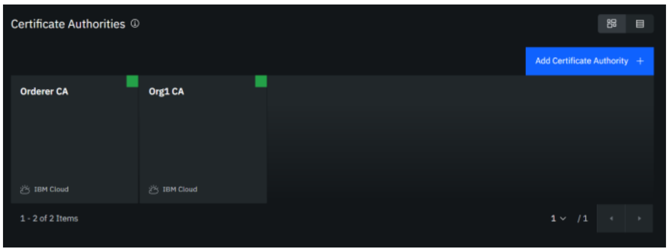


III.VI.II Certificate Authorities

The Blockchain network serve as a series of managed communication between nodes to serve a defined business use case. For these communications to authenticate (to ensure, in other words, who is who,ie to recognise the nodes) requires identities and a whole system of permissions that can be verified during each interaction.

In Hyperledger Fabric, the IBM Blockchain Platform, this property is the Certificate Authority (CA), which forms identities in the form of x509 certificates as well as define whole of an organization through the creation of a Membership Services Provider (MSP), which defines the permissions of identities at a channel and component level. These identities can include attributes about them, for example, by linking them to a organizational unit (OU) or a particular organization .

An organization MSP(Membership Service Provider), has an MSP subfolder called admins. Any user whose certificate identity is inside that admin folder is an admin of the organization. Because this MSP(Membership service provider) defines the organization or the department, it is listed in the configuration on every channel which consists the network of which the organization is a member. As a result, whenever an head or the admin of the organization tries to perform any action, the signing certificate or identity of the admin (which is attached to all of its communication) is verified against the certificates listed in the membership service provider. it is checked that the certificate match the one listed in the channel configuration? If it does match then the other organizations will authenticate it and the action can be performed. If not, the request to perform the action is declined.

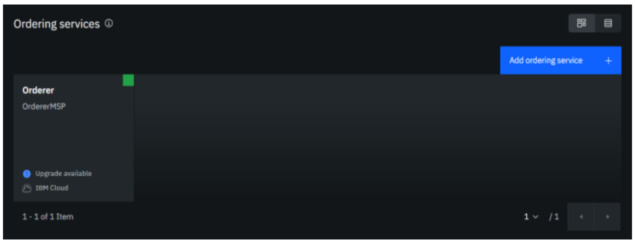


III.VI.III Ordering Services

Hyperledger Fabric features a kind of a node that relies on deterministic consensus algorithms that is called an orderer, also known as an “ordering node”, that does this transaction ordering. The collection of ordering nodes form the "ordering service".

In addition to promoting final steps, separating the endorsement of smart contract of blockchain execution (which happens at the peers) from ordering gives

HyperledgerFabric advantages in performance and scalability, efficiency, eliminating bottlenecks that can occur when execution and ordering are performed by the same nodes.The ordering service performs one other key function: it maintains what is known as the "system channel", a default channel that consists the network that hosts a "consortium", it is the list of organizations that can create and join the application channels.



III.VI.IV Channels

A channel which consists of a network is a mechanism that facilitates a private layer of communication, allowing subsets of network members to create a separate ledger for their transactions. Channels consisting of a network are not just private in the sense that network members who are not subjected to any of the channel are unable see the interaction, they are also secret in the sense that unless a network member is a part of the channel, they will not even know that the channel exists. The IBM Blockchain Platform allows channels to be easily created and managed. Channel consisting of a network configuration updates allow the members of a channel consisting network to edit channel parameters to fit their use case. For example, more nodes can be added to a channel which consists the network, or the capacity and ability of a channel can be changed. Because changes to a channel must be approved by members who are a part of that channel, the IBM Blockchain Platform has a procedure for the collection of necessary and important signatures.

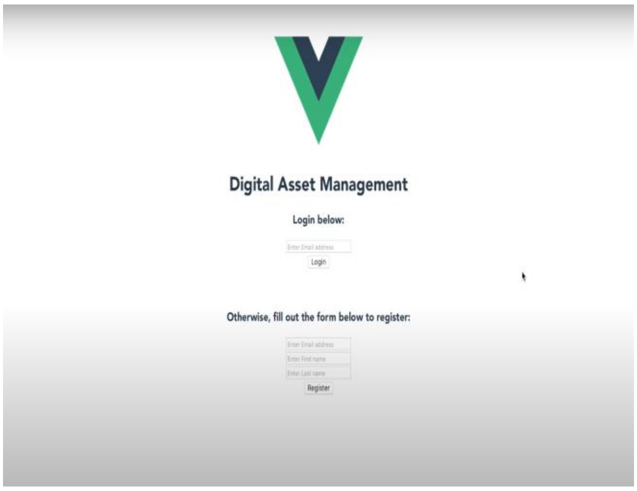
III.VI.V Smart Contracts

A smart contract in a blockchain network defines the rules and regulations between different organizations or departments in executable code. Applications call a smart contract to generate transactions that are stored or saved on the ledger or database.

Using a HyperledgerFabric blockchain network, we can turn these smart contracts into executable programs – known in the organization as **smart contracts** – to open up a whole new wide variety of new possibilities. That's because smart contracts can implement the governance rules or regulations for **any** type of business object, so that they can be simultaneously performed when the smart contract of a blockchain network is executed. For example, a smart contract of a blockchain network might ensure that a new car delivery has to be made within a specified timeline, or that funds are released according to prearranged or predetermined terms, improving the flow of goods or capitals respectively. Most importantly however, the execution of a smart contract is much more efficient and convenient and is impervious against all the errors which occur in manual human business processes. Hyperledger fabric provides various language support for writing smart contracts or chaincode, which provides great flexibility in creating applications.

IV. RESULTS

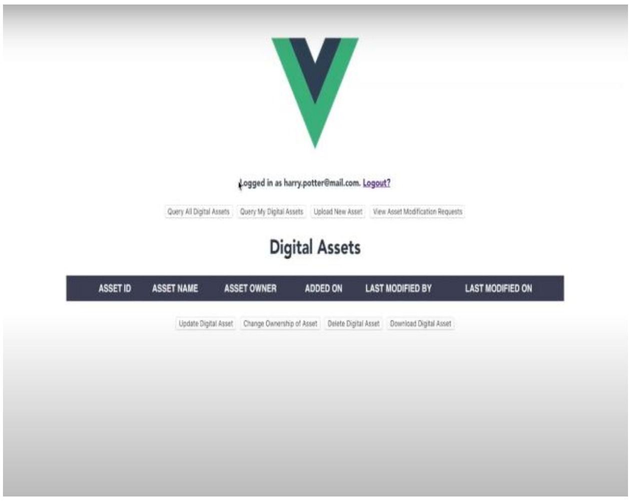
In this project we have used HyperLedger Fabric as a blockchain platform to build our project. In this project we have ensued various security layers. In Hyperledger Fabric, with the help of channels the network is secured from external threat. Blockchain in itself is secured as a network. In the website, where we have connected the site to the blockchain platform is also secured, we have achieved this by using various industry level hashing algorithms. The use case of this project is that in a particular organization or in a department, user can upload, delete, update, change ownership of the asset. Such as given in the below figure that is presented.



Digital Asset Management

Login below:

Otherwise, fill out the form below to register:



Logged in as harry.potter@mail.com. Logout?

Digital Assets

ASSET ID	ASSET NAME	ASSET OWNER	ADDED ON	LAST MODIFIED BY	LAST MODIFIED ON

V. CONCLUSION

Using blockchain frameworks, we successfully built a highly secure and scalable system for storing, updating, deleting and transferring digital asset management with next to 0 cost for development. Using open source technologies, multiple organizations and governments can implement their own private blockchain network for secure and reliable data management needs.

VI. FUTURE WORK

Integrating with the government and providing licensing. Providing legal rights (enforce registrations/copyrights). Smart contracts can be used to automatically release funds when a certain objective is accomplished. Providing digital certificates, Validating integrity of song/art/design or any other asset. Digital transfer of IP assets (transferring ownership).

REFERENCES

1. Uri Jocobovitz, "Blockchain for Identity management", Technical Report #16-02, The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University, Beer Sheva, Israel, 2018.

2. Blockchain Identity Management: The Definitive Guide(2021 Update), https://tykn.tech/identity-management-blockchain/

3. Suporn Pongnumkul, Chaiyaphum Siripanpornchana, Suttipong Thajchayapong, “Performance Analysis of Private Blockchain Platforms in Varying Workloads,” September18, 2017

4. Luca Foschini, Andrea Gavagna, Giuseppe Martuscelli, a Rebecca Montanari, “Hyperledger Fabric Blockchain: Chaincode Performance Analysis,” 27 July, 2022