International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Document Management using Private Permissioned Blockchain.

Shriyash Shingare[1], Neel Khalade[2], Raghav Saoji[3], Avadhoot Dhanve[4], Dr.Uma Pujeri

[1,2,3,4]Trimester 9,School of Computer Engineering and Technology, MIT World Peace University, Pune,
[5]Associate Professor, School of Computer Engineering and Technology, MIT World Peace University, Pune

---

Abstract - *As we are living in the 21st century, we are still using the 19th century mechanisms for managing a user's identity. Although there are some improvements in the last couple decades where man has tried to digitalize documents. By doing so, it has reduced a lot of overheads & redundant work. But as digitalized world also has negative side, the security of a user's information is highly questioned. As there are many new solutions for solving these issues, still technology is lacking behind in gaining trust of society & thus a digital identity is now not trusted, is reverified to obtain whether the identity exists in the real world. There are better solutions like using some type of blockchain technologies, but the beginning of the blockchain was started with hiding digital identity & having a digital currency which was used for all sorts of illegal things & didn't build a good reputation to the general public. In my research I have made a summary of existing technologies used in India & proposed a solution which is absolute in many aspects by using private permissioned blockchain with the support of Hyperledger fabric. Where the data which is stored is stored on servers of multiple authorities & services can only access an individual's information by users consent for time requested. The data can be accessed only by the API which my service will provide & only by the users consent to share information.*

Key Words:**KYC, UIDAI Aadhar, Permissioned Blockchain, Hyperledger Fabric, Data Privacy, Data Ownership**

1.INTRODUCTION

Innovation has improved a great deal in ongoing decades; the PC appearance have completely changed the way people live, work and play. Organizations grow in a highly productive way, with the help of PC. Thusly, it has diminished a ton of overheads and repetitive work. However, as digitalized world additionally has negative side, the security of a client's data is exceptionally addressed. Although in documentation companies speak to that they are taking all the measures they can and could, there are information breaks which has scrutinized man's conviction that is his/her computerized character is secure? As there are numerous new answers for explaining these issues, still innovation is missing behind in picking up trust of society and subsequently an advanced personality. These issues have driven establishment for making numerous methods of arrangements like UIDAI's Aadhar[1] for India and numerous nations creating comparable arrangements like these have recently found

1/10 of the answer for the issue is currently not trusted, is reverified to acquire whether the personality exists. There are better arrangements like utilizing blockchain innovations, yet the start of the blockchain was begun with concealing computerized personality and having an advanced cash which was utilized for a wide range of illicit things and did not construct a decent notoriety to the overall population. These days, as some rumoured associations like the Linux establishment and IBM[2] began planning utilizing blockchain began a transformation in individuals comprehend of the blockchain. In this way, I likewise will in general make novel answer for these issues of advanced character the executives, KYC[1] and archive the board by utilizing private permissioned blockchain.

Digitization is a way of converting data into a computer (for example a virtual PC), where the data is sorted into bits. The result is the display of an object, image, sound, record, or symbol (usually a simple symbol) by creating a continuation of numbers that indicate a different arrangement of focus or test. The outcome is called computerized portrayal or, more explicitly, an advanced picture, for the item, and advanced structure, for the sign. In current practice, the digitized information is as paired numbers, which encourage PC preparing and different activities, in any case, carefully, digitizing basically implies the change of simple source material into a mathematical organization; the decimal or whatever other number framework that can be utilized.

1.1 Blockchain

A blockchain is a distributed system for recording history of transactions on a shared ledger, providing *consistency* (i.e., all participants have the same view of the ledger) and *immutability* (i.e., once something is accepted to the ledger, it cannot change). First known as crypto-currencies such as Bitcoin [7], blockchain technology today is gaining ground in some areas, and it has been suggested by some that disruptive innovations such as open source software [6] or the Internet [8]. Hyperledger Fabric [4] is an approved contract, in which letter writing requires certain trust. Participants who are allowed to write a ledger on the Hyperledger Fabric are called peers (and usually only a few). This setting makes it easier to control the actions of the ledger, and is usually faster than the public blocks used in most crypto-currencies. Nearly all blockchain architectures

support the notion of *smart contracts[11]*, namely a programmable application logic that is invoked for every transaction. In the Hyperledger Fabric, these smart contracts are made with chain code [11], which can be a counter system (Go), created by (some) peers. The chain code has access to the current logger and details of the new transaction, and determines whether that transaction will pass or not, as well as data added to the ledger.

1.2Why Hyperledger Fabric?

Build on permissions Hyperledger Fabric [4] comes with a full license system. You can choose who will have access to your blockchain and what level they reach. So basically different players see things differently. This is not possible in Ethereum.

Aspect	MultiChain	Public blockchains	Hyperledger	ChainCore
Cost	Infrastructure only	Cost for each transaction	Infrastructure only	Infrastructure only
Permission administration	Different permission settings	Each user individually	Different permission settings	Different permission settings
Privacy options	Both public and private	Public only	Both public and private	Both public and private
Compatibility	Compatible with bitcoin core	Usually not compatible with more blockchains	Not compatible with more blockchains	Not compatible with more blockchains
Consensus	"MiningDiversity "	Proof-of-work	PBFT	Federated Consensus Protocol
Availability of information	Available only with user permissions	For all the users of the blockchain	Available only with user permissions	Available only with user permissions

Fig1 Comparative table of blockchain platforms considered

2. Proposed Solution

we have decided to use Hyper-ledger Fabric for building our use case. for solving the issue in the document sharing system. So, I propose to build a solution where-

2.1.1 Organizations can define documents.
Organizations can build their own documents means that they can create a custom document using in built service where they can define the fields of document that organization needs.

2.1.2 Then, users can view these documents & fill these documents if it as defined like that, or an organizations can directly add entries to a user's information with the users consent.

2.1.3.Simple & Easy to use API
we proposed to build an API which is lot simpler to use and share document, system can handle all the necessary things required for setting up the Hyperledger & keeping in mind that user can write simple API calls for requesting for a document, creating a document, adding a entry in documents & also for giving consent for using a particular type of document. Simpler UI on a website where users will be able to invoke the same type of API where they can easily set up new documents & manage UAC (User Access Control)

2.1.4 Users can track & trace usage of their information We tend to create a simple user interface at the user side, where citizens or the person using my system can get a seamless experience. Keeping Indian moto in mind, we want to develop a website which supports all major languages used in India the whole idea emphases upon maximum people can use our platform. the whole idea emphases upon maximum people can use my platform. On the platform, users will be able to control all the information that they share to the outer world also give access to different organizations to view the information also they can revoke the granted access after a certain period of time or anyhow they want to.

2.1.5 Scalable Approach[8] In terms of approach, Hyperledger Fabric is itself build upon Docker Composers, So we want to make use of that where our service will be able to scale all the resources when it's having user to a 100ds of millions of users so that we could conserve the resources and also the cost of scaling can be efficiently managed. We want to build the APIs which can scale, we will develop our solution in NodeJS, as it is a single threaded language and can be asynchronously written where the server won't have to wait until the information is retrieved properly.

Roles of a user –

2.1. Upload a particular document-

Here, a user can select the type of document the user wants to upload on the platform. The user will be given a large list of documents where he can just select the document he tends to upload. Then automatically, the fields required for the document would be retrieved & user can fill up that information. This information is then passed on to the responsible authority for that document, then that authority has the right to approve or disapprove the information filled.

2.2. Give services access to the document information

When a particular organization asks for documents, user can decide whether he/she wants to share their information. So, a particular user has access to edit the information, depends upon whether the organization wants user to edit the information. So, basically a user has to access over the information he/she has uploaded, there can be some information which user is also not allowed to edit like editing Birth Certificate, college degree etc. But a user can select whom to share that information and from whom to decline the request, which brings us to our next point.

2.3. Revoke access given to the services-

By revoking the access, the information stored in the database at the organization side will be deleted. However, the ledger information in a particular transaction will not get deleted. So, we can only find that the event of sharing that information happened, but that organization will not be able to access the data as it will get deleted. So, a transaction will stay recorded, but the actual data will not be there on the organizational side.

2.4. Trace every document & see who is using my information

Users will be able to trace the log of information, so he/she can basically have the access to the complete ledger information associated with their account. Will also have a live view where they can see how many are accessing their information now in Realtime.

2.5. What organizations can do? 1. Define new documents

1. The organizations will be able to create new documents by simply calling the API or by using the UI platform.
2. To create a new document, the organization will have to specify their org_id so the service can track that which user created the document.
3. Can define documents fields with the simple API like-

1. createDocument (service_unique_id, unique name, [concerned users], title: '<-text->', description: '<- text->', ...fields)
field = {label:'', placeholder:'(if any)', defaultValue:'', typeOfValue: <number>, <text> etc} d. In such way, a new document can be easily created & managed by the organization who owns it.

2. Approve uploaded documents **a.** A particular organization will be able to approve the data provided by its users, they can also decline & raise a query. The organization can also specify in the API that whether the users can change the information or no.

3.Store documents transactions on ledger
1. A particular organization can store all the transactions on their ledger which can be referenced when needed.

Fig 2. Different document issued to person

a. requestDocument(service_id, user_id, document_id)
b. The organization can request a particular document from the user when needed, that can be simply done by invoking the API or by theUI

Table -1: Comparison of existing technologies.

"Digital Locker" Technology Specification (DLTS) Version 2.3, March 2015 https://img1.digitallocker.gov.in/assets/img/technical-specifications-dlts-ver-2.3.pdf	Decentralized implementation of digital document storage, Uses Ethereum smart contracts for user control Has distributed file system storage database	1. Uses centralized database, which can be vulnerable to other natural hazards. 2. Built system is not scalable for the Indian population to use. 3. Chances of document forgery if documents not properly verified	1. Needs to have a scalable and distributed ecosystem Document uploading needs to be restricted, and document assignment to users should be promoted.
DOCS TRACK - DOCUMENT MANAGEMENT SYSTEM Volume: 05 Issue: 01 | Jan-2018 e- ISSN: 2395-0056	Document management service based on user's consensus	1. Limits to only management system, must be implemented as blockchain Not scalable to handle changing requests.	1. Can be further developed by implementing the gaps, i.e. by having microservices architecture Using private permissioned blockchain for managing documents
Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference Association for Computing Machinery, New York, NY, USA, Article 30, 1–15. DOI: 10.1145/3190508 ISBN: 9781450355841 April 2018 https://doi.org/10.1145/3190508.3190538	Is a distributed operating system which uses microservices based architecture, which can be built to be scalable. Implemented a true framework for private permissioned blockchain	1. Difficult to implement using an easy api. 2. Setting up ecosystem is complicated	1. Can implement usingthis technology but needs to have easy to use api for users Onboarding of new organization can be simplified.

3. CONCLUSIONS

Data security is one of the major advantages of blockchain technology. Blockchain is a large open-source online application where each node stores and verifies the same data. This blockchain-based system will provide completely secure storage of the document over the internet by keeping it safe from being tampered by any third person. Also, it will provide 100 percent availability of e-document as and when required by the owner of that particular e-document.

We Can Build A Complete Solution Which Is Truly Based on The Digital Information. Less Bad for Environment Building Scalable, Modern & Sustainable Solutions Can Reduce Business Costs. Blockchain Based Totally Immutable Solutions Are the New IndustryStandard. Blockchains Security, Privacy, Traceability, Inherent Data Provenance and Timestamping Has Seen Its Adoption Beyond Its Initial Application Areas. Using Hyperledger Fabric We Can Build Application for Any Use Case We Want

ACKNOWLEDGEMENT

This research was supported by MIT World Peace University. The authors would like to thank the Department of Computer Science and Technology, Faculty of Computer Science and Technology, Dr. Uma Pujeri, MIT World Peace University, Pune, India , for providing facilities and guidance.

REFERENCES

[1] Dixon, P. A Failure to “Do No Harm” -- India’s Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.. Health Technol.7,539–567(2017). https://doi.org/10.1007/s12553-017-0202-6

[2] F. Benhamouda, S. Halevi and T. Halevi, "Supporting private data on Hyperledger Fabric with secure multiparty computation," in IBM Journal of Research and Development, vol. 63, no. 2/3, pp. 3:1-3:8, March-May 2019, doi: 10.1147/JRD.2019.2913621

[3] Savić, Dobrica. (2019). From Digitization, through Digitalization, to Digital Transformation. 43/2019. 36-39

[4] Zhong, B., Wu, H., Ding, L. et al. Hyperledger fabric-based consortium blockchain for construction quality information management. Front. Eng. Manag. (2020). https://doi.org/10.1007/s42524-020-0128-y

[5] Parra Moyano, J., Ross, O. KYC Optimization Using Distributed Ledger Technology. Bus Inf Syst Eng 59, 411–423 (2017). https://doi.org/10.1007/s12599-017-0504-2

[6] Satpathy, T. The Aadhaar: “Evil” Embodied as Law. Health Technol. 7, 469–487 (2017). https://doi.org/10.1007/s12553-017-0203-5

[7] “Digital Locker” Technology Specification (DLTS) Version 2.3, March 2015 https://img1.digitallocker.gov.in/assets/img/technical-specifications-dlts-ver-2.3.pdf

[8] DOCS TRACK -DOCUMENT MANAGEMENT SYSTEM Volume: 05 Issue: 01 | Jan-2018 e-ISSN: 2395- 0056

[9] Official Hyperledger Docs - https://hyperledger-fabric.readthedocs.io/

[10] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf , Dec 2008

[11] Canhui Wang, & Xiaowen Chu. (2020). Performance Characterization and Bottleneck Analysis of Hyperledger Fabric. https://arxiv.org/abs/2008.05946

BIOGRAPHIES

B-Tech, School of Computer Engineering and Technology, MIT World Peace University, Pune,

B-Tech, School of Computer Engineering and Technology, MIT World Peace University, Pune,

B-Tech, School of Computer Engineering and Technology, MIT World Peace University, Pune,

B-Tech, School of Computer Engineering and Technology, MIT World Peace University, Pune,