AN IDENTITY MANAGEMENT SYSTEM USING BLOCKCHAIN

Prathamesh Patil[1], Divya Bharambe[2], Mandar Chaudhari[3], Satish Kuchiwale[4]

[1-3]Students, Dept. of Computer Engineering, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India.
[4]Asst.Professor, Dept. of Computer Engineering, Smt. Indira Gandhi College of Engineering, Navi Mumbai, Maharashtra, India.

Abstract: The Internet these days needs a distinguishing protocol for figuring out human creatures and organizations. As a result, organizations had to develop and keep their databases of consumer data. This reply is sumptuous to the organization, inefficient as a bounty of the data is copied all through the special organization, intense to steady as proving through current large-scale private records breaches over the world, and bulky to the clients who need to do not disregard one of a kind units of qualifications for special administrations. Moreover, private information can be collected for records mining, profiling, and misuse without customers' know-how or assent. The man or woman presents proof of identification and club through sharing appropriate components in their identification with the carrier organization. This overview seriously explores one of a kind blockchain-primarily based completely on identification control and verification frameworks.

Keywords: **Blockchain, Ethereum, Smart Contracts, Metamask, IPFS.**

I. INTRODUCTION

Since the last decade, humans have begun to realize the importance and difficulty of Internet security. Personal data is being exploited or disclosed regularly, and economic belongings are at risk, among other things. Internet users are harmed directly or indirectly by these incidents of data security, and in a few cases, the entire Internet transaction atmosphere is destroyed. As a result, each Internet group and educational student is trying to find ways to manipulate an online identification. Several efforts have been made to ensure the safety of personal information. The opposite is true when it comes to personal information, which is usually stored on a centralized server, making it simpler for hackers or attackers to accomplish their dangerous goals by stealing, misusing, or changing this information. Blockchain Identity Management offers a decentralized and steady answer through a dissipated acceptance of the paradigm. The answer places humans back in control. The most important feature of the Blockchain is its decentralization, meaning that each node in the community is responsible for maintaining the full database. Consensus ensures that each node, or a majority of nodes, agrees on the technology and the extrusion of statistics. At each turn, you will be required to provide a variety of government-issued identification cards, including a voter ID and passport, pan card. As several IDs are shared, privacy risks and statistics breaches arise. As a result, the blockchain can facilitate self-sovereign identity through decentralized networks that enable the authentication of private information via the means of securing identification papers, verifying identification files, etc and Using permissioned participants to endorse identification files.

II. BLOCKCHAIN

In the context of Blockchain Technology, otherwise known as Distributed Ledger Technology (DLT), this refers to the era where decentralised databases were used to manipulate records among entities through a peer-to-peer network, a consensus algorithm makes sure the replication takes place on all nodes in the network.

The blockchain [14] is an immutable, distributed ledger that has the capability to record data about transactions and assets on a network. As a result, increasingly more costs can be tracked and traded on a blockchain network, decreasing hazard and lowering costs for all parties involved. Assets can be tangible (a house, a car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

III. TECHNOLOGIES

Ethereum

Blockchain technology provides developers with the ability to develop and share business, financial, and entertainment applications.A decentralized blockchain platform is a platform that establishes a peer-to-peer community for executing and verifying utility codes, also known as smart contracts [14]. Smart contracts allow members to transact with each other without relying on any central authority. Each member has access to transparent, verifiable, and immutable transaction statistics, giving them full control over and visibility into transaction data.Ethereum users pay costs to utilize dApps. Transactions are sent through and obtained by Ethereum accounts [14]. To signal transactions, a sender spends Ether, the local cryptocurrency of Ethereum, as a value of processing the transaction at the

community.Since the costs range depending on the amount of computational electricity needed, they are referred to as "gas."

Ethereum Smart Contracts

The Ethereum blockchain is used to run "smart contracts". They are made up of code (functions) and data (states) and are stored at specific addresses on the Ethereum network.

As mentioned above, smart contracts [1] are a type of Ethereum account; they have a balance, and are capable of sending payments over the network. But smart contracts are not controlled by a user, instead, they run as code when deployed to the network. Smart contracts [14] can also act as contracts and define rules. They have the functionality of a regular contract, but they can enforce rules based on the code. Interactions with smart contracts are irreversible and cannot be reverted.

Ganache

It is a platform that allows you to develop, deploy, and test your apps in a safe and deterministic way. Ganache is based on Ethereum and Corda and allows you to develop, deploy, and test your applications in a deterministic and safe way.

IPFS

IPFS (InterPlanetary File System) is a protocol and peer-to-peer community with an allotted document system for storing and sharing content. IPFS uses content-addressing to uniquely identify each document in an international namespace that connects all computing devices. A cryptographic hash of IPFS files may also be saved on a blockchain. However, IPFS no longer permits users to proportion documents with other parties. When sharing sensitive or non-public information, this is required.

Metamask

It is a software program that allows you to interact with Ethereum blockchains using a cryptocurrency wallet. It provides users with access to their Ethereum wallets through a browser extension or mobile app, so they can then interact with decentralized applications via the wallet. A blockchain software firm, ConsenSys Software Inc., developed MetaMask by specializing in Ethereum-based mostly equipment and infrastructure.

How does Blockchain work?

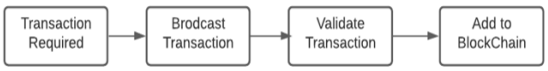

Fig 1. Blockchain Transaction Process

An individual might request a transaction. The information may be about cryptocurrency, contracts, facts, or something else. Using nodes, the asked transaction is broadcast to a P2P community. Users and users' fame are confirmed by a community of nodes using recognized algorithms. As soon as the transaction is complete, the new block is added to the existing blockchain. In this way, the transaction is permanent and immutable.

IV. METHODOLOGY

Blockchain technology has been at the heart of our project. We've constructed our system on top of the blockchain. The system will be used by two people one as an individual, and the second as an organization. Signing in to the system will allow one to add the documents and make transactions through metamask. To make transactions, we use Ganache which generates sample accounts with Ethereum coins loaded in them. Smart contracts are embedded in this account. The smart contracts [1] are written in a solidity programming language. All functionality is embedded within smart contracts.

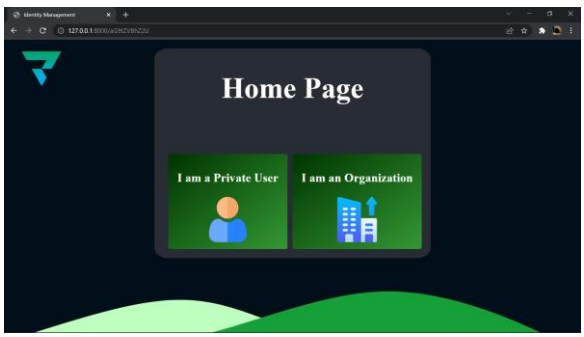

Fig 2. Home Page

To use our system, users and organizations must register on our system, for which they need to enter their email address, after which they will receive a one-time authentication code to their email address. Following that, they will be redirected to generate a password. All user credentials and organization credentials will be stored in the cloud and the password will be encrypted in the cloud using hashing. In IPFS [16], documents are saved as hashes. Once the transaction has been approved, the hashes will be stored on the blockchain.

With IPFS, one can create a permanent and distributed web that utilizes a content-based address instead of HTTP's location-based address.

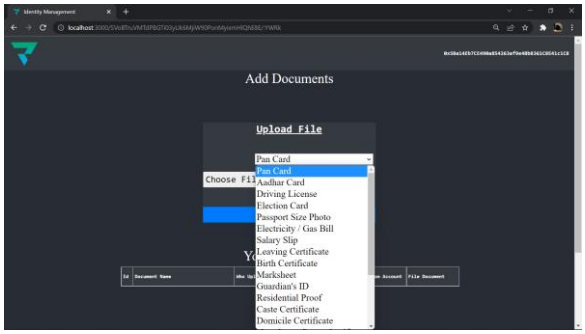

Fig 3. Add Document Page

An HTTP request would look like http://10.20.30.40/folder/file.txt.

An IPFS request would look like /ipfs/QmT5NvUtoM5n/folder/file.txt

The IPFS protocol uses a cryptographic hash of a file to address content instead of a location address. This is done using a cryptographic hash on the file. The hash represents a root object, and all objects along its path can be accessed through it. Rather than talking to a server, you gain access to this "starting point" of data. Using this method, the system leverages physical proximity. If a person very close by has what I want, I may get it directly from them without having to connect to a central server.

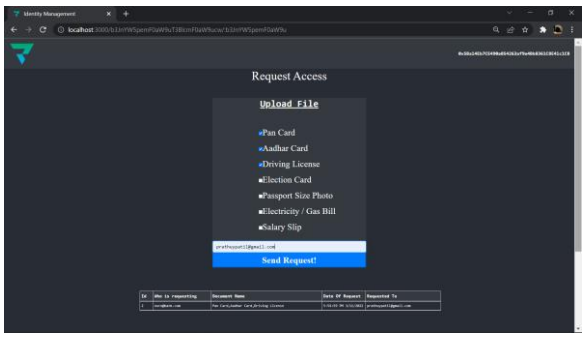

Fig 4. Organization Request Access

With IPFS [16], data is stored using Distributed Hash Tables or DHTs, which we obtain from peers. After we establish a hash, we ask the peers whose content is located at that hash, and we download the data directly from that peer. A mechanism similar to BitTorrent transfers data between nodes in the network.

Afterward, the organization will request the person for the documents they need. Upon the person's approval of that request via a transaction [1], the organization will gain access to those documents.

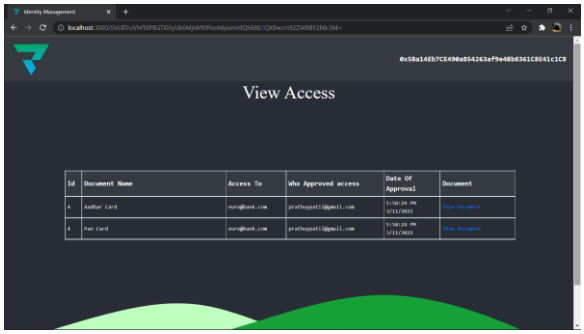

Fig 5. View Document Access

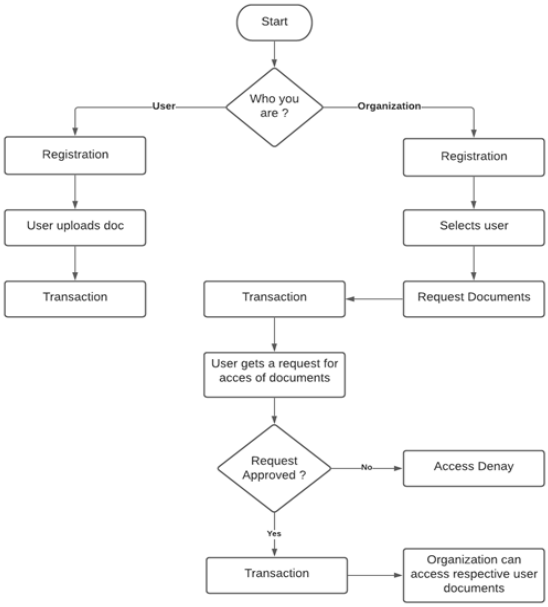

Fig 6. Flow Chart for Identity Management

Data Segregation

As the application relies on identity management, the user uploads the documents. Depending on the type of organization, the documents will be classified. For instance, a list of documents required by the bank will appear only against the respective user if the organization is a bank, and the bank can request access only to the relevant documents.

Data Immutability

A system based on blockchain prevents the data from being deleted or altered. Therefore, if a user uploads a document, it cannot be deleted or changed. As an organization can only request the newly updated document of the user, If any changes or corrections are made to a document that was previously uploaded, the user can upload the updated document again.

V. RESULT

When the person uploads the files, the organization requests the files it needs to confirm. After receiving a request from the organization, the person approves the files he wants to transmit and the company grants him access. As a result, the organization will easily be able to access the files and confirm the person's identity. There is no need for any paperwork or to put up xerox copies of the documents. This results in a faster way for the company to confirm an employee. Furthermore, by utilizing the blockchain era the individual will no longer have to go to an organization to upload their files. The technology ensures both the person's safety and the safety of the organization.

VI. CONCLUSION

We present in this paper a project for designing an independent identity management system based on Blockchain technology; we introduce the main working principles of the project and discuss the identity authentication system. By using the identity authentication model, we clarify how the organization is allowed to access the user's documents based on their permissions. Finally, we conducted a set of experiments to test the feasibility of the proposed module, and the results were satisfactory. In the coming years, we plan to conduct large-scale real-time experiments using real data in the public Ethereum system to further enhance and improve it.

VII. REFERENCES

[1] Yuan Liu, Zheng Zhao,Guiding, GuoXingwei Wang, Zhenhua TanShuang Wang"An Identity Management System Based on Blockchain"2017 15th Annual Conference on Privacy, Security and Trust

[2] Raju, S., Boddepalli, S., Gampa, S., Yan, Q., & Deogun, J. S. (2017). Identity management using blockchain for cognitive cellular networks. 201v7 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2017.7996830

[3] Gilani, Komal; Bertin, Emmanuel; Hatin, Julien; Crespi, Noel (2020). [IEEE 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) - Paris, France (2020.9.28-2020.9.30)] 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) - A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal

[4] Gururaj, P. (2020). Identity management using permissioned blockchain. 2020 International Conference on Mainstreaming Blockchain Implementation (ICOMBI). doi:10.23919/icombi48604.2020.9201137–1149, 2017.

[5] Zhang, M., Wang, S., Zhang, P., He, L., Li, X., & Zhou, S. (2019). Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption. 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). doi:10.1109/itnec.2019.8729244

[6]Kuperberg, M. (2019). Blockchain-Based Identity Management: A Survey From the Organization and Ecosystem Perspective. IEEE Transactions on Engineering Management, 1–20. doi:10.1109/tem.2019.2926471

[7] Zhu, X., & Badr, Y. (2018). A Survey on Blockchain-Based Identity Management Systems for the Internet of Things. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), and IEEE Smart Data (SmartData). doi:10.1109/cybermatics_2018.2018

[8] Xiaoyang Zhu, Youakim Badr" A Survey on Blockchain-based Identity Management Systems for the Internet of Things"2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybernetics.

[9] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Transactions on Wireless Communications, vol. 10, no. 2, pp. 431–436, 2010.

[10] C. Chang and H. Tsai, "An anonymous and self-verified mobile authentication with an authenticated key agreement for large-scale wireless networks," IEEE Transactions on Wireless Communications, vol. 9, no. 11, pp. 3346–3353, 2010.

[11] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena. (2017) Uport: A platform for self-sovereign identity. Accessed on: Nov. 2019.

[12] Sovrin. Accessed on: Nov. 2019. [Online]. Available: https: //sovrin.org

[13] ShoCard. Accessed on: Nov. 2019. [Online]. Available: https://shocard.com [14] N. Lo and J. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319–1328, 2015.

[14] Zheng Zhao and Yuan Liu: A Blockchain-based Identity Management System Considering Reputation," 2019 IEEE 2nd International Conference on Information Systems and Computer-Aided Education (ICISCAE) 978-1-7281-3066-8/19/$31.00 ©2019 IEEE

[15] Samia El Haddouti and M. Dafir Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology," 978-1-5386-8317-0/19/$31.00 ©2019 IEEE

[16] H. Gunasinghe and E. Bertino, "PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 1042– 1057, 2018.