AN IDENTITY MANAGEMENT SYSTEM USING BLOCKCHAIN: A SURVEY

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

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

Abstract: The Internet nowadays lacks an identification protocol for figuring out human beings and organizations. As a result, organizations had to construct and keep their personal databases of consumer data. This answer is luxurious to the organization, inefficient as plenty of the data is duplicated throughout the unique organization, tough to stable as evidenced through current large-scale private records breaches across the world, and bulky to the customers who want to don't forget unique units of credentials for unique services. Furthermore, private data can be accrued for records mining, profiling, and exploitation without customers' know-how or consent. The best answer could be self-sovereign identification, a brand new shape of identification control, this is owned and managed completely through every man or woman consumer. This answer could encompass the man or woman's consolidated virtual identification in addition to their set of confirmed attributes which have been cryptographically signed through numerous depended on issuers. The man or woman presents evidence of identification and club through sharing applicable components in their identification with the carrier organization. This survey severely investigates unique blockchain-primarily based totally on identification control and authentication frameworks.

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

I. INTRODUCTION

The significance and problem of Internet protection had been introduced to humans note in the last decades. Personal statistics are regularly exploited or disclosed, and economic belongings are compromised, amongst different things. These protection incidents bring about direct or oblique monetary damages for Internet users, and in a few cases, the complete Internet transaction atmosphere is destroyed. As a result, each Internet group and educational student are grappling with a way to manipulate an online identification. Many efforts had been made to discover powerful strategies to make certain the safety of private statistics. Personal statistics, on the alternative hand, is usually saved in a centralized server, making it simpler for hackers or attackers to meet their dangerous functions via way of means of stealing, misusing, or changing these statistics. Through a dispensed acceptance as true with the paradigm, Blockchain Identity Management offers a decentralized and steady answer that places humans returned in control.

The maximum vital detail of the Blockchain is its decentralization, this means that each node withinside the community is answerable for retaining the complete database. A consensus technique guarantees that each one node or a majority of nodes agree on the technology and extrude of statistics. At each turn, you may be required to perceive yourself the usage of numerous government-issued identity cards, which includes a voter ID, passport, or Pan Card. Privacy dangers and statistics breaches stand up whilst several IDs are shared. As a result, the blockchain can lead the manner to self-sovereign identity through decentralized networks that make certain privateness accept as true via way of means of securing identification papers, verifying identification files, and endorsing identification files via way of means of permissioned participants.

II. BLOCKCHAIN

Distributed Ledger Technology (DLT), usually virtually called “Blockchain Technology”, refers back to the era at the back of decentralized databases imparting manipulate over the evolution of records among entities through a peer-to-peer network, the use of consensus algorithms that make certain replication throughout the nodes of the network.

Blockchain [14] is a shared, immutable ledger that permits the technique of recording transactions and tracking assets in an organization’s network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually something of the cost may be tracked and traded on a blockchain network, decreasing hazard and slicing prices for all involved.

III. TECHNOLOGIES

Ethereum

Ethereum is an open-source blockchain platform that develops and shares business, financial services, and entertainment applications.

It is a decentralized blockchain platform that establishes a peer-to-peer community that securely executes and verifies utility code, referred to as smart contracts. Smart contracts [14] permit members to transact with every different without relying on valuable authority. Transaction statistics are immutable, verifiable, and securely allotted throughout the community, giving members complete possession and visibility into transaction data. Transactions are despatched from and obtained through user-created Ethereum [14] accounts. A sender has to signal transactions and spend Ether, Ethereum's local cryptocurrency, as a value of processing transactions at the community. Ethereum customers pay costs to apply dApps. The costs are referred to as "gas" due to the fact they range relying on the quantity of computational electricity required.

Ethereum Smart Contracts

A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.

Smart contracts [1] are a type of Ethereum account. This means they have a balance and they can send transactions over the network. However they're not controlled by a user, instead, they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts [14] can define rules, as a regular contract, and automatically enforce them via the code. Smart contracts can not be deleted by default, and interactions with them are irreversible.

Ganache

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. You can use Ganache across the entire development cycle; enabling you to develop, deploy, and test your apps in a safe and deterministic environment.

IPFS

The InterPlanetary File System (IPFS) is a protocol and peer-to-peer community for storing and sharing facts in an allotted report system. IPFS [16] makes use of content-addressing to uniquely perceive every report in an international namespace connecting all computing devices. It is based on cryptographic hashes which can without problems be saved on a blockchain. Nonetheless, IPFS no longer allows customers to percentage documents with decided parties. This is necessary if touchy or non-public facts desire to be shared.

Metamask

MetaMask is a software program cryptocurrency wallets used to have interaction with the Ethereum blockchain [14]. It permits customers to get admission to their Ethereum wallets through a browser extension or cell app, that could then be used to have interaction with decentralized applications. MetaMask evolved via means of ConsenSys Software Inc., a blockchain software program corporation specializing in Ethereum-primarily based totally gear and infrastructure.

How does Blockchain work?

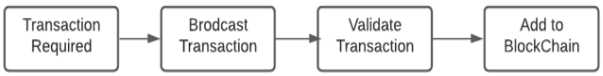

Fig 1. Blockchain Transaction Process

Some individuals request a transaction. The transaction can be concerned with cryptocurrency, contracts, facts or different information.

The asked transaction is broadcasted to a P2P community with the assistance of nodes. The community of nodes validates the transaction and the user's fame with the assistance of acknowledged algorithms.

Once the transaction is complete the brand new block is then brought to the prevailing blockchain. In this sort of manner, this is everlasting and unalterable.

IV. METHODOLOGY

The methodology of our project is primarily based totally on blockchain technology. Using blockchain we've got constructed our system. The system will be utilized by folks one is the person and the second is the organization. The person will sign in on our system and will add the documents. While uploading the documents the person will need to make a transaction through metamask. For

transactions [1], we make use of ganache which gives sample accounts with ethereum coins loaded in it. This account is linked with the smart contract. The smart contracts [1] are written in a solidity programming language. All this functionality is written in smart contracts.

The documents of the person are saved in IPFS [16] which returns a hash. When the person completes the transaction and approves it, the hash will be saved in the smart contract.

IPFS seeks to create a permanent and distributed web. It does this by using a content-addressed system instead of HTTP's location-based system.

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

Instead of using a location address, IPFS [16] uses a representation of the content itself to address the content. This is done using a cryptographic hash on a file and that is used as the address. The hash represents a root object and other objects can be found in its path. Instead of talking to a server, you gain access to this "starting point" of data. This way the system leverages physical proximity. If someone very close to me has what I want, I'll get it directly from them instead of connecting to a central server.

To store data, IPFS [16] uses a Distributed Hash Table or DHT. Once we have a hash, we ask the peer network who has the content located at that hash and we download the content directly from the node that has the data I want. Data is transferred between the nodes in the network using mechanisms similar to BitTorrent.

Then the organization will request the person for the files they need. Once the person approves the request by making a transaction [1] the respective organization will get access to that document.

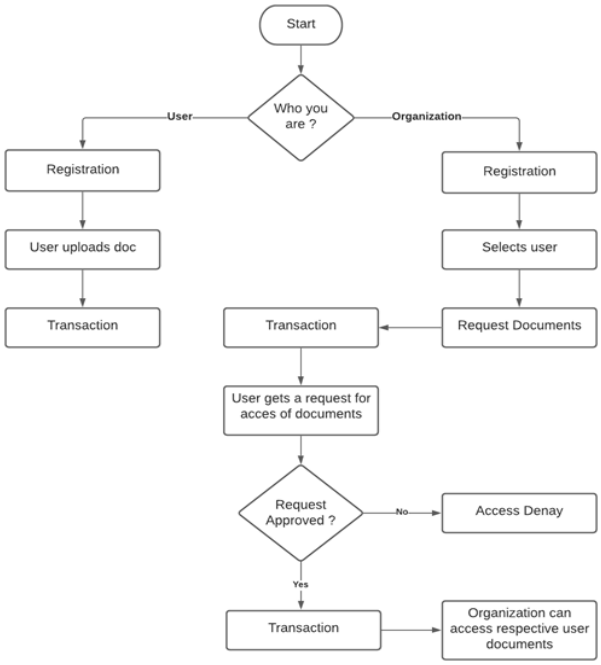

Fig 2. Flow Chart for Identity Management

V. RESULT

The person uploads the files then the organization requests the files they need to affirm. The person receives a request from the organization then the files to which he approves the files to which he desires to supply get admission. Thus the organization will effortlessly get admission to the files and may affirm the person. There isn't any want for any documentation paintings or to put up any xerox copies of the files. This results in a quicker technique for the organization to affirm any person. Also, the person will now no longer need to go to the organization to put up the files. Using blockchain era ensures protection and protection for the organization in addition to the person.

VI. CONCLUSION

In this paper, we planned an identity management system using Blockchain. We introduce the working principle of the project and discuss the identity authentication model. In the identity authentication model, we clarify how the user's documents are uploaded and accessed by the organization through the user's permission. Finally, we checked the feasibility of the system by conducting sets of experiments, and the experimental results satisfied the proposed module. In the future, we plan to conduct large-scale real data-based experiments in public Ethereum to further improve the proposed system 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.