iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44335

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

Blockchain-based Self-sovereign Identity Management System

Gauri Shetye[1], Nandini Sonar[2], Dr. Dhanamma Jagli[3]
[1,2]*Final year Student,* [3]*Assistant Professor, Dept. of M.C.A, V.E.S. Institute of Technology, India*

Abstract - The whole concept of self-sovereign identity (SSI) is gaining a lot of optimism, with the emerging Blockchain Technology in the current tech-scenario. It is a major change in how online interactions will take place in the future considering the identity of each user. The different aspects of SSI are examined by various works in the literature This paper surveys the origin of identity, various digital identity models and how it leads to self-sovereign identity. It then goes on to discuss related research, as well as the SSI's building blocks, which include decentralized IDs, verifiable credentials, a distributed ledger, and a variety of privacy mechanisms. Finally, it proposes a solution for self-sovereign identity by using the Ethereum platform for blockchain and other technologies
***Keywords - Blockchain, Self-Sovereign, Identity, Ethereum, Smart* Contracts, IPFS**

I. INTRODUCTION

The processes and technology used in an organisation to identify, authenticate, and authorise a user to access the resources or systems of a certain entity or other affiliates is known as Identity management. Customers or employees accessing software or hardware within an organisation, the amount of access, rights, and restrictions each user has, the issuance and identification of birth certificates, national identity cards, travel documents or driver's licences, as well as other documents that allow users to confirm their identity and access services from the government or any other administration, and so on.

A. Problems with the current Identity Management Systems

There's a problem with identity. It's subject to loss, theft, or fraud if it's on paper, such as birth certificates kept among other documents in a government office. By allowing for greater interoperability across departments and other organisations, a digital identification eliminates paperwork and speeds up processing inside these administrations. However, storing this digital identity on a centralized server makes it vulnerable to unauthenticated users. The majority of today's identity management systems are insecure and outdated. Identities must be portable and verifiable wherever, at any time, and digitalization makes this possible. However, being digital is insufficient. Privacy and security are also important considerations for identities.

B. Industries that have difficulties with current identity management systems include:

Government: The lack of interoperability between governance departments and other entities has a negative impact on all aspects of government. This, in turn, raises the time and cost of the process.
Healthcare: More than half of the world's population lacks access to adequate healthcare. The absence of interoperability among workers in healthcare institutions (hospitals, small clinics, insurance facilities, doctors, pharmaceutical companies, and so on) results in inadequate care, delayed assistance, and increased patient irritation.
Education: The difficulty in approving and verifying student credentials leads to the hiring of unqualified applicants and the tarnish of the schools, colleges, and employing businesses' brands.
Banking: Using login credentials such as passwords makes banking transactions less secure for users.
Businesses in general: Storing the data of clients and employees is a cause of legal liability for businesses. Clients' trust may be lost as a result of breaches of confidential and personal information, and the company's brand may suffer as a result.

C. Models Systems of Digital Identity

The first digital identity model system involves an organisation providing a person with a valid digital identity in order to grant them access to its services. Every new organization with which a person wishes to interact needs the creation of a new digital identity. As a result, one will have a negative user experience. The user must keep track of all the sites on which he has registered and create new passwords and credentials every time.
The "Federated" model of digital identity management is the second model system. Due to the poor user experience with the original system, third-party organisations began offering digital identification credentials that allow consumers to access a variety of different services and websites. The services "Login with Facebook" and "Login with Google" are excellent examples of this paradigm. Companies outsource their identification systems to huge corporations with a financial stake in large databases

of personal information, such as these. This raise worries about privacy and security. Facebook, Google, and others become trusted intermediaries.

With the emergence of Blockchain technology, Decentralized Identifiers, and Verifiable Credentials, a third type of identity known as Self-Sovereign Identity can now be created.

II. SELF-SOVEREIGN IDENTITY MANAGEMENT SYSTEM

Verifiable Credentials, Decentralized Identifiers, and blockchain or Distributed Ledger are the three foundations of Self-Sovereign Identity.

Verifiable Credentials, which combine PKC (public-key cryptography) and privacy-increasing approaches to prevent correlation, allowing digital watermarking of claimed data. As a result, not only can physically safe credentials be converted to digital, but users of these credentials can also choose what information they want to share, such as specific information from the credential without revealing the original data (proving your age without an ID card), and third-party organisations can verify this data instantly without having to contact the issuer.

Decentralized Identifiers are global identifiers that are both unique and permanent. They have complete influence over the owner of the identity. Unlike centralised registration systems, organisations, or identity suppliers, DIDs are self-contained.

When a person receives a Verifiable Credential, the administration assigns their Public DID to these credentials. The same Public DID is also stored on the blockchain, which is an immutable database. When someone wishes to verify and authenticate this Credential, they may look up the DID on the blockchain to determine who the issuer is without having to contact the issuing company. The Blockchain serves as a verifiable data register that anybody may use to confirm the organisation associated with the Public DID. A distributed ledger in SSI management systems allows everyone in a network to know the same truth if a credential is trustworthy and who authorized the validity of the data inside that credential without revealing original data.

A. Owners, Issuers, and Verifiers are the Three Actors in SSI with Blockchain.

It's crucial to understand the three different entities who play a part in identity systems when discussing blockchain technology: identity owners (users), identity issuing entities, and identity verification entities.

The identity issuing body, such as the local government, must be a trusted party that can give personal credentials to an identity holder. The identity issuing entity validates the personal data in the credential by issuing it. These credentials can be saved in the identity-owning user's own identity wallet and used to establish their identity to a verifying entity afterwards.

A credential is made up of several attributes, and an identity attribute is information on the owner's identity (name, age, birth date). The usefulness and dependability of this certificate are entirely dependent on the granting organization's trustworthiness and repute.

B. What role does SSI play in Reducing Privacy and Security Concerns?

The verifying organisations can use blockchain to examine the authenticity of the credentials and issuing organisation from which they can decide whether to authenticate this proof instead of having to verify the validity of the raw data in the proof supplied.

E.g. Instead of worrying about the truth of the birth date itself, when an identity-owning person provides proof of their birth date, the verifying organisation will validate the government issued signature to this credential and then make a decision whether to trust the government about the data's accuracy. As a result, proof validation is reliant on the verifiers' assessment of the issuer's trustworthiness.

Without actually keeping any personal or sensitive information on the blockchain, blockchain fosters trust between companies and ensures the legitimacy of data and identifiers. This is critical because a distributed ledger like blockchain is immutable, which means that anything we place on it can never be changed or erased, hence no sensitive data should ever be stored on it.

III. TECHNOLOGIES

A. Ethereum

Ethereum is a distributed computing platform based on blockchain that allows developers to create and deploy SSI-based decentralised applications. It creates a peer-to-peer community that runs and validates smart contracts, which are utility programmes.

Smart contracts allow network members to transact with one other without having to worry about their authorization. The statistics of these transactions are irreversible, verifiable, safe, and distributed throughout the community, giving network participants total visibility and access to transaction-related data. User-created Ethereum accounts are used to send and receive transactions. To conduct transactions in the Ethereum community, a sender must sign a transaction and spend Ethereum's local

cryptocurrency, Ether, as a value. Customers of Ethereum must pay a fee to use dApps (Decentralized Applications). Because it is based on the amount of computational electricity spent, the cost which is referred to as "gas."

B. Ethereum Smart Contracts

On the Ethereum blockchain, a Smart Contract is a code that executes. It's a set of functional programs and data stored at a single Ethereum blockchain address. It is installed on the network and begins to function as expected. The Ethereum account is linked to the smart contract. It has a balance and can send transactions via the network. The user has no control over it. User accounts can engage with a smart contract by inputting transactions that perform the smart contract's functionality. Smart contracts, like conventional contracts, have rules that are written and enforced automatically through code. Smart contracts are unchangeable, and their interactions are irreversible.

C. Ganache

Ganache is a virtual blockchain that can be used to quickly construct Ethereum applications. It allows you to create, deploy, and test your apps in a secure and predictable environment.

D. IPFS

The InterPlanetary File System (IPFS) is a protocol and peer-to-peer network for storing and exchanging information in a designated report system. IPFS uses content addressing to ensure that each report is uniquely perceived by all computers in the network. It is based on cryptographic hashes that may be stored on a blockchain without difficulty. . IPFS no longer allows users to percentage documents with decided organizations. This is necessary if touchy or non-public facts are desired to be shared.

E. Metamask

Metamask is a cryptocurrency wallet that interacts with the Ethereum network. Customers can utilise this browser extension to access their Ethereum wallets, which can then be used to interact with decentralised applications. Metamask is a product of ConsenSys Software Inc., which is a blockchain software programme corporation that specialises in Ethereum infrastructure.

IV. METHODOLOGY

The blockchain technology is at the heart of our Self-Sovereign Digital Identity system. Users and businesses can both benefit from the system. The user will login and add his identification documents to the system. The user will have to conduct a transaction through Meta mask while uploading these documents. We'll utilize Ganache for transactions, which provides sample accounts loaded with Ethereum cryptocurrency. The smart contract is then linked to this account. These smart contracts are created in the Solidity programming language and have all of the functionality.

The user's documents are saved in IPFS, which returns a hash value. The hash will be stored in the smart contract once the user has completed and approved the transaction.

Instead than using HTTP's location-based approach, IPFS uses a content-addressed mechanism to establish a distributed and permanent network..

http://1.2.3.4/folder/abc.pdf is an example of an HTTP request.

/ipfs/ZjU7DcOkyB2n/folder/abc.pdf is an example of an IPFS request.

Instead of a physical address, IPFS addresses the material using a representation of the material itself. This is accomplished by utilising cryptography to generate a hash on a document and using it as the address. There is a root item in the hash, as well as other objects that can be located along its path. Instead of connecting to a server, the user connects to the data's beginning point. The system makes use of physical proximity in this way. Instead of linking to a central server, if someone very close in proximity to the user has what the user wants, the user will acquire it straight from them.

The data is stored in PFS using a DHT (Distributed Hash Table). Once the user knows the hash value, they can contact the peer network that has the material at this hash, and the user can retrieve the data straight from the node that has it. Data is exchanged between nodes in the network using processes similar to those used by DigiLocker.

The organisation might make a request for the papers they require from the user. Once the user authorises the request by completing a transaction, the requested papers will be made available to the appropriate organisation. The company can then validate these documents and issue the user with digital identity credentials. These credentials are attested to the blockchain. Instead of the original documents, the user now has an unchangeable and portable identity that may be used for further verifications.

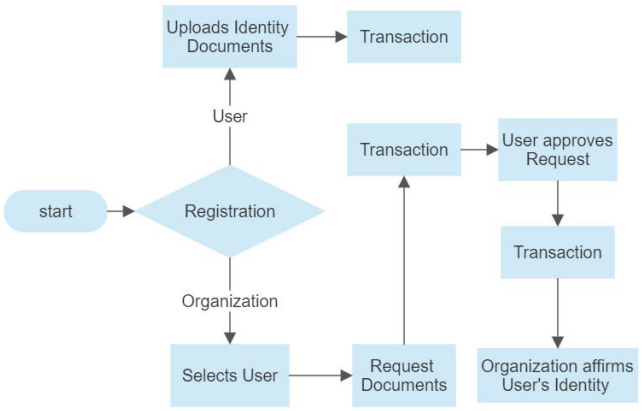


Fig. 1 Flow Chart

V. RESULT AND CONCLUSION

In this work, we ideate a solution for a Blockchain-based system for self-sovereign identity management. The user submits the documents, which are subsequently requested by the organisation in order to authenticate the person's identification. The user receives a request from the organisation, to which he responds by approving the documents to which he want to grant access. As a result, the organisation will have easy access to the papers and will be able to verify the user. As a result, the organisation has a simple process to confirm any user. Furthermore, the user will no longer be required to physically visit the company in order to post any documents. For both the corporation and the user, the blockchain generation ensures privacy and security.

REFERENCES

[1] Kaliya Young and Heather Vescent, "A Comprehensive Guide to Self-Sovereign Identity" April 6, 2019

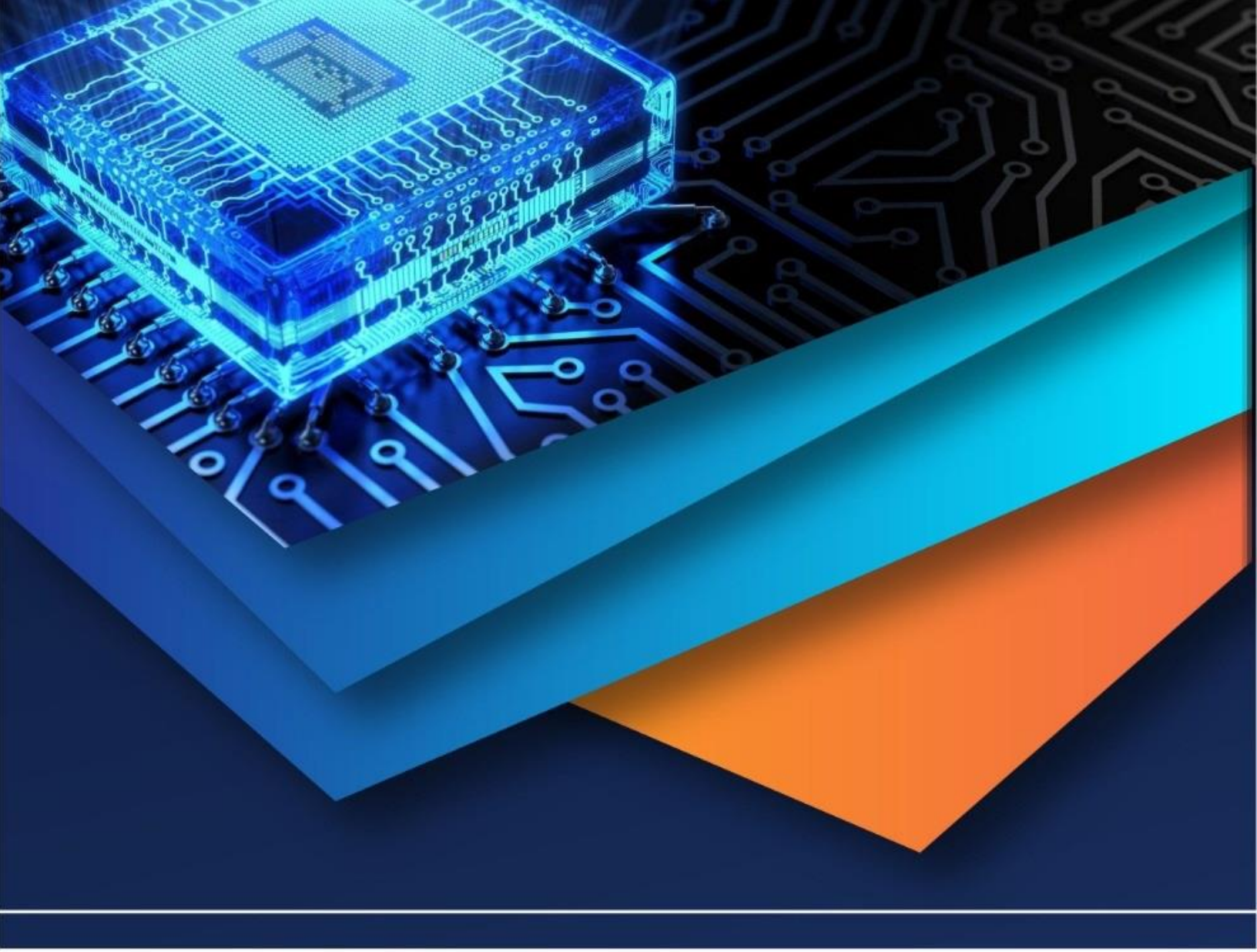
[2] Christopher Allen, "the-path-to-self-sovereign-identity" lifewithalacrity.com April 25 2016

[3] 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

[4] [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

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

[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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY