Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 4s (2024)

Decentralization of Identity using Ethereum and IPFS

Shailaja Lohar[1], S. D. Babar[2], P. N. Mahalle[3]
[1]Smt.Kashibai Navale College of Engineering, Pune,India
shailaja.lohar@gmail.com
[2]STES'S Sinhgad Institute of Lonavala, Pune, India sdbabar@sinhgad.edu
[3]BRACT's Vishwakarma Institute of Information Technology,
parikshit.mahalle@viit.ac.in
Pune, India

Article History:
Received: *18-04-2024*
Revised: *12-06-2024*
Accepted: *25-06-2024*

Abstract:
Introduction: The Identity of a user in digital world is an important factor for an individual. Identity management has been handled by various models which, over the period of time have been prone various security breaches. The foremost integral part of any identity model is the centralized storage, access of data. Considering this, in recent years, there has been evolution from centralization to de-centralization of Identity management. With respect to this new aspect, this paper proposes a solution to the centralized management problems, as a decentralized Identity Management System. The said approach utilizes Ethereum blockchain, IPFS, both supporting distributed data accessibility and data storage respectively. This paper also sheds light on the W3C specification of DID (De-centralized Identifier) which supports the Self-Sovereign Identity principles of Identity Management and are vital for de-centralization of Identity Management

Keywords: SSI, IPFS, ZKP, Zk-SNARK, Ethereum, Metamask

1. Introduction

Identity Management systems are crucial for any individual to exist in digital world. To assist the users in managing these digital identities, there have been different types of Identity Management models as mentioned in [14].

Authentication and Verification processes have been integral part of Identity Management Systems. The entities involved in this process are Issuer, Holder and Verifier. For traditional Identity Management System, the main concern and limitations arise from the centralized nature of Identity Management [8]. Overcoming these drawbacks has been a part of many researches. [mention my paper with SSI]. The inclination towards adaption of new Identity model "SSI" is growing in recent years. Decentralization, Identity ownership, are the strongest factors of SSI which eliminate the dependency of third party centralized verifiers for authentication. To develop such systems, Distributed Ledger Technology (DLT) is used, which works in completely decentralized environment.

Blockchain Technology comes into picture when DLT is to be used for any application. Bitcoin [11] was the first application based on Blockchain introduced by Satoshi Nakamoto. Ever since, it has evolved into a plethora of applications in various domains. Blockchain has also been widely used in Identity Management applications [8]. In this we paper we propose a solution to identity management based on SSI principles for the use case of authentication and verification of Identity of a user by storing his passport details but verifying his age without revealing the other personal details.

The main contributions of the paper are as follows:

- Proposed new Identity Verification system based on SSI principles.
- Use Ethereum Blockchain and Smart Contracts for verification of Identity.

- Identity Verification is kept Anonymous with Zero Knowledge Proof.

In remainder of the paper, section II gives overview of existing literature, section III explains the layered architecture and brief introduction to the technologies used. Section IV describes the working of the system along with the algorithms. Section V shows the results and analysis and section VI concludes the paper with future enhancements.

2. Related Work

In the past few years, there have been SSI-based identity management projects built on the DLT. The niche for these projects is the Blockchain, which offers benefits like immutability, de-centralization, transparency and auditability.

Gruner et al [1], presents a framework as a quantifiable trust model for blockchain-based Identity management system. The authors give a simplified and automated trust model for which they have assumed claims and attestations of an SSI to derive a trust value for the claims.

Tom Hamer et al [2], present a unique SSI, with combination of Biometric and W3C[17] to allow user to have at most one shared instance of his digital identity proof and avoiding multiple enrolments without user permission. One key of improvement though, can be work on integrity of shared data.

Lee et al [3],presents a blockchain based SSI IdM framework, which uses zero-knowledge proofzk-Snark[19]. Their system, gives a faster verification. [add more]

X Wang et al [4] present an Identity management system which uses zk-snark algorithm to improvise the system in blockchain and avoid exposure of ownership of attributes. Their system allows selective disclosure of ownership related attributes with zero knowledge proof.

Vanga et al[5], proposes identity management using consortium Blockchain and using biometrics of user for authentication. The authors claim this to be the protocol, first of its type as providing privacy to identity information which is stored on blockchain.

S. Hong et al, [6], presents a SSI based identity model using OAuth procedure for authentication and authorization. The model is user supported and avoids the multiple ownership of identity.

Shang Gao et al [7], presents a novel identity authentication method utilizing Blockchain-based privacy safeguards. Users autonomously generate identity data and complete certification via Blockchain Technology. This approach mitigates storage burdens associated with storing numerous certificates or key pairs. It eliminates single point failure.

Ahmed et al [15], proposed a decentralized identity management system based on Hyperledger Indy Blockchain for public transportation. They aim to eliminate multiple travel cards and give users more control of their digital identity and is based on SSI principles.

Reza et al[16], present a paper that sets foundation for digital client on-boarding system utilizing Hyperledger Indy and SSI principles. Through this initiative, the authors aim to tackle challenges like the issues where IDm Models overlook the user as primary stakeholder, and address fragmentation of user's digital identity data across multiple providers. The approach proposes the user's control over digital data and new digital approach to KYC process.

Barros et.al [21], presents a system architecture designed for issuing and verifying VCs using SSI to providevaccination proof. The Blockchain used by the Authors is Hyperledger Indy for the SSI implementation. It generates a VC with vaccination information, ensuring a high level of privacy through selective disclosure and ZKP. For verification, biometric are used for authorizing the vaccinee , as well as verfiers' biometrics is used.

Singh et. al [22] propose a privacy-preserving credential scheme on the blockchain that enables users to anonymize their attribute values and communicate non-interactively with certificate and service providers. Hyperledger Fabric is used Attribute values are anonymized in both off-chain and on-chain communications to

ensure anonymity. Verification is done using elliptic curve-based non-interactive Schnorr proof of knowledge for the correctness of commitment and the blind version of the user's secret key

Javed et al [23], present a blockchain-based decentralized identity management system that allows patients and healthcare providers to identify and authenticate themselves transparently and securely across different eHealth domains. Patients and healthcare providers are uniquely identified by their health identifiers (healthIDs). The identity attributes are attested by a healthcare regulator, indexed on the blockchain, and stored by the identity owner. We implemented smart contracts on an Ethereum consortium blockchain to facilitate identification and authentication procedures. The authors also suggest their future use of IPFS storage.

S.Wang et al [24] , we propose a cloud user identity management protocol based on the Ethereum blockchain, along with a framework for a simple credit management system. This new protocol is an enhanced version of CIDM (Consolidated Identity Management), called EIDM (Ethereum-based Identity Management) protocol. The improved protocol incorporates JWT (JSON Web Token) in OAuth 2.0 to introduce smart contracts into the EIDM protocol, and includes a credit management system to provide a reliable identity authentication protocol for cloud users and service providers. This new protocol addresses the issue of over-reliance on third parties in existing identity management solutions.

Xia et al [25] propose a Digital City Operating System, which collect user attributes and securely transmit them to other system components for verification. Upon successful completion of the verification process, a digital identity is created for the applying resident and the set of transactions leading to the ID creation are stored in the blockchain. Authors implemented the blockchain framework on a Ethereum blockchain network

Yang et al[26], This paper incorporates zk-SNARK into the existing claim identity model to enhance identity privacy. We design a privacy attribute token and two specific computations to enable the secret transfer of privacy attribute ownership and authenticate attribute ownership. The proposed BZDIMS utilizes a framework of off-chain computing and on-chain verification, effectively preventing the exposure of the ownership link between user entities and attributes on the distributed ledger. This approach ensures identity unlinkability and behavior privacy.

S. Friebe et al [27], propose DecentID, a decentralized identity storage system based on Ethereum smart contracts. DecentID eliminates the need for a single trust anchor, protects the privacy of user identity data, and allows users to create multiple identities from subsets of their stored attributes, such as addresses, photos, or videos. Despite being decentralized, the system enables users to manage their attributes and identities in one place. This means users only need to trust a verifiable system rather than relying on the benignity of an identity provider. To protect user privacy, access to identities and attributes by services is restricted and must be granted by the user, ensuring users maintain control over their identity data. The authors combine blockchain with external storage organized as a key-value store, such as a distributed hash table (DHT). Using cryptographic data stored on the blockchain, we ensure the integrity of identity data in the external storage.

3. Gap Analysis

The Digital Identity Management has undergone many technological developments over the period of time. Traditional Identity management systems [18] have escalated from centralized approach of user authentication to de-centralized, through User-centric to Federated systems. As mentioned in section II, there has been research on integrating Blockchain into Identity Management. Using de-centralized platform to store identity related data can be expensive in terms of storage as well as computation. Further, to comply with requirements of SSI principles and W3C specifications, we need a mechanism to create a Universal unique id to identify the user in digital space. Some of the important factors in de-centralizing Identity Management are listed below.

1. A distributed system for eliminating drawbacks of centralized identity storage
2. Time optimization with respect to accessing Identity related data without Issuer overhead.
3. Controlled revelation of Identity.

The above gaps lead to the proposed system in this paper which uses Ethereum Blockchain, IPFS(Interplanetary File System) and zero-knowledge proof.

Motivation

Identity management system's evolution has been on rise from web 1.0 to web 4.0. The earliest version being the User centric Identity management systems, followed by Federated systems, which gave the user's the privilege to login to multiple domains through single Identity authentication, but, this approach faced major drawbacks, in terms of threats related to mutlidomain attacks and phishing attacks. The shift in Identity Management paradigm, with the advent of SSI, has given advantages over multiple issues faced by traditional Identity management systems. Giving user the complete authority of his Identity, and addressing the threats to IDM system, is the major reason for the shift to decentralized approach from centralized. The issues addressed and mitigated by de-centralized IDM can be listed as follows:

1. Third party Verifiers are eliminated in de-centralized approach
2. The least, the Identity data is shared, least are the chances of theft, attacks and misuse of the Identification.
3. Immutability of the Identity data is of importance, since digital world has expanded in direct proportion to vast number of users.
4. Scalability is important due to growing number of digital users, the system for Managing the Identity must be consider this as an important need.

These issues highlight the need of De-centralized Identity management and the SSI approach for need of new Identity management system. This paper proposes an Identity management approach, motivated to resolve the mentioned issues of IDM system, which complies with some of the SSI principles [10], and uses the smart contracts, Blockchain, IPFS for a use case of age verification along with selective disclosure.

4. Fundamental Terminologies

Ethereum Blockchain

Blockchain technology is a form of distributed ledger technology. As a decentralized system, it offers an immutable processing environment for applications. It organizes recorded data into interconnected blocks, while distributed ledgers enable the recording, sharing, and synchronization of transactions across independent computers in their digital records. Ethereum is an open blockchain network that allows individuals to participate and utilize decentralized applications (dApps), which are developed and operate on the Ethereum Virtual Machine (EVM).

The primary entities within the Ethereum ecosystem include:

1. Ether: This is Ethereum's native cryptocurrency, referred to as ether or ETH. It is exchanged between user accounts and is also utilized to cover transaction fees, known as gas, which are incurred for computational operations.
2. Accounts: Ethereum features two distinct types of accounts. Externally Owned Accounts (EOAs) are managed via private keys, granting their holders the authority to send ether and messages from these accounts. On the other hand, Smart Contract Code Controlled Accounts possess their own executable code and are governed by this code.

Smart contracts are programs typically coded in Solidity or Vyper. These programs are compiled into bytecode for the Ethereum Virtual Machine (EVM) and operate on the Ethereum blockchain. Each smart contract is deployed to a unique address on the blockchain and comprises both code, which includes multiple functions, and data, representing its state. Smart contracts can establish rules and autonomously enforce them through their code. Users interact with smart contracts by initiating transactions that execute specific functions defined within the contract.

Zk-SNARK

Zero-knowledge proof are pivotal in blockchain-driven identity management systems, ensuring transaction privacy, user authentication, and the sharing of verifiable data. By employing zero-knowledge proofs, credentials can be disclosed to verifiers only in the required context by hiding the other relevant information.
The abbreviation zk-SNARK stands for:
Zero-knowledge – conceals the details of knowledge.
Succinct – the proof verified in milliseconds, with a compact proof size of only a few hundred bytes.
Non-interactive – involves a single message sent from the prover to the verifier, rather than a sequence of exchanges.

Self-Sovereign Identity (SSI) empowers individuals with control over their digital identities in a decentralized manner. SSI represents a novel approach to identity management where users maintain full authority over their identity data without external intervention. Different entities participate in the SSI process, as depicted in Figure 1. For instance, during a transaction, one party submits credentials to others, who then verify the credentials' legitimacy by confirming they originated from a trusted issuer. The trust the verifier places in the issuer is subsequently conveyed to the credential holder.

Christopher Allen[10] and the reputable team at Metadium5, both prominent in the SSI credential-based systems domain, have highlighted the absence of a universally accepted definition for SSI. SSI starts with a digital "wallet" housing digital credentials. This wallet mirrors a physical counterpart where individuals store credentials issued by others, such as passports, bank authorizations, or academic certificates. However, these digital credentials are digitally signed, enabling cryptographic verification of three key aspects to any verifier:

- Identity of the issuer
- Recipient of the credential
- Integrity (whether it has been tampered with since issuance)

SSI can be defined as ten guiding principles, which was categorized into three sections: Security, Controllability and Portability [12], [13]. Transparency and Access, viewed solely from the perspective of the identity owner, guarantee that individuals can use their identities whenever and wherever they choose.

Security	Controllability	Portability
Keep identity information secure	Users must take control of their data,e.g who can see or access	Users can utilize their identities wherever they want, without being tied to any provider
Protection Persistence Minimisation	Existence Persistence Control Consent	Interoperability Transparency Access

Fig. 1 SSI Categorization

W3C specification
The W3C (World Wide Web Consortium) is an international community that develops open standards to ensure the long-term growth of the web. They create specifications for web technologies, ensuring interoperability and accessibility across different platforms and devices.
W3C has been actively involved in efforts to standardize technologies related to decentralization, including decentralized identifiers (DIDs) and verifiable credentials. These specifications are essential components for building decentralized identity systems.

1. Decentralized Identifiers (DIDs): DIDs are a new type of identifier that enables verifiable, self-sovereign digital identities. They are designed to be fully under the control of the DID subject, independent of any centralized registry, identity provider, or certificate authority. The W3C has published the "Decentralized Identifiers (DIDs) Specification" to define the syntax and semantics of DIDs, as well as the methods for creating, resolving, and managing them. This specification enables interoperability between different decentralized identity systems.

2. Verifiable Credentials: Verifiable credentials are digital credentials that can be cryptographically verified by relying parties. They enable individuals and organizations to securely present and verify claims about themselves, such as identity attributes, qualifications, or permissions, without the need for a central authority. The W3C has developed the "Verifiable Credentials Data Model" and associated specifications to standardize the format, structure, and cryptographic mechanisms for creating and verifying verifiable credentials. This includes specifications for JSON-LD-based data models, cryptographic suites, and presentation formats.

5. Proposed Methodology

These specifications provide the foundation for decentralized identity systems that prioritize privacy, security, and user control. They enable individuals to manage their own digital identities, share verifiable information selectively, and interact with various services and applications without relying on traditional centralized identity providers.

The figure 2. Shows the Proposed Methodology along with the important components contributing to the de-centralized system .The following algorithms show the implementation scenario of the system. Also, the complete system Architecture is depicted in figure 8.

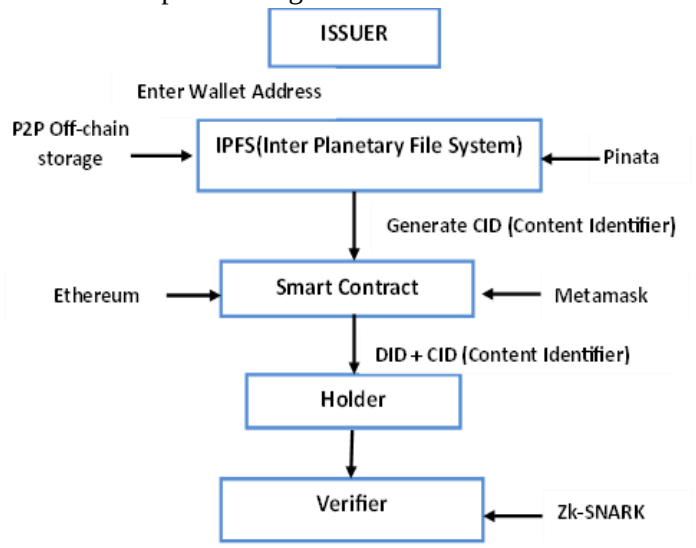

Fig.2 Proposed Methodology

Any user or “Holder”, has an identity and its attributes, which will be stored in and its CID (Content Identifier) generated by IPFS will be used to generate the unique DID for the user.

Algorithm (1) : Holder
Input: Check for user registration
Output: Fetch Credentials
Step 1: Connect to a wallet through Metamask
Step 2: Fetch wallet address
Step 3: Check if the address is linked with any user.
Step 4: If user not registered, then goto “Issuer”
Step 5: If user is registered, then “Fetch Credentials”
Step 6: Stop

The screenshot shows the wallet address connected to the Holder, and whether the credentials are stored

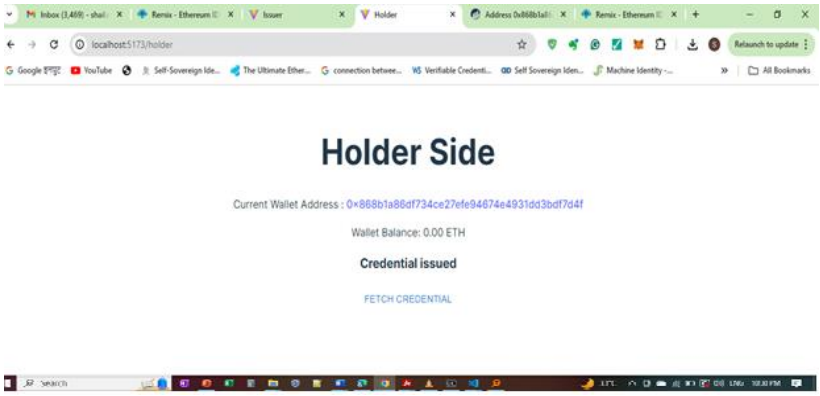

Fig.3 Wallet address connected to Holder

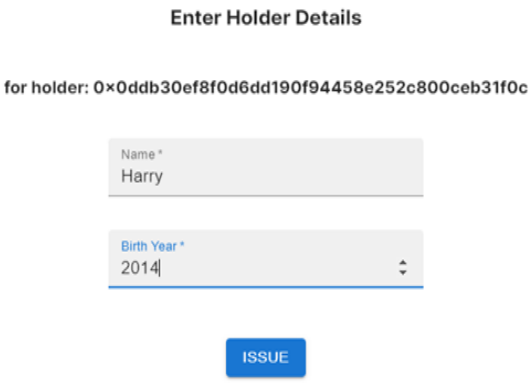

Fig. 4. Storing details of user

Algorithm (2) : Issuer
Input: Wallet address of Holder
Output: DID of user
Step 1: Select the wallet address
Step 2: Enter Holder details
a. Enter Name
b. Enter Birthyear
Step 3: Call mint() function to create DID
Step 4: DID is generated for the given wallet address
Step 5: Stop

The Issuer part has two options, one which shows the DID Issued Holders and the other with only a wallet but no DID.

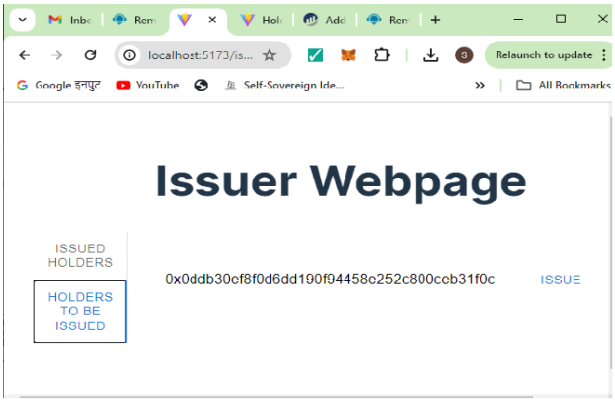

Fig. 5. DID Issued and to be Issued

The following algorithm shows the Verification process, where DID is checked and if it is created , the ZKP algorithm is invoked, else the user is prompted to create the DID first.

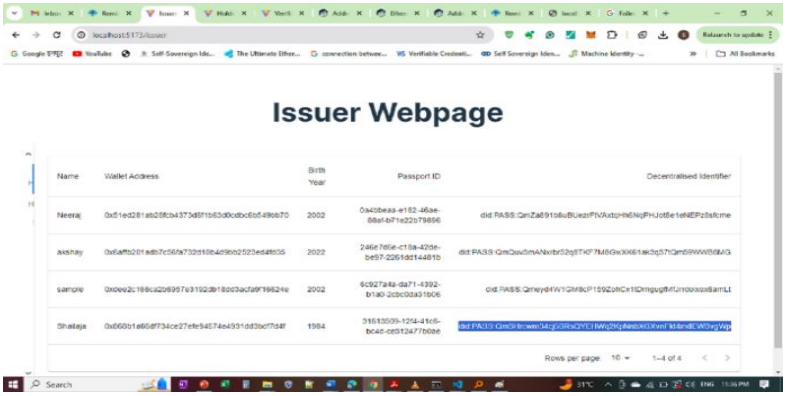

Fig.6. DID Issued details

After entering the Name and Age details of the Holder, a DID is generated in the format: did:PASS:QmSHrcwm34cj5BRsQYEHWq2KpNnbXGXvnFkt4mdEWBvgWp

This ID is used further by Verifier, to check, whether the Holder of the Identity is a User above 18 years of age or below.

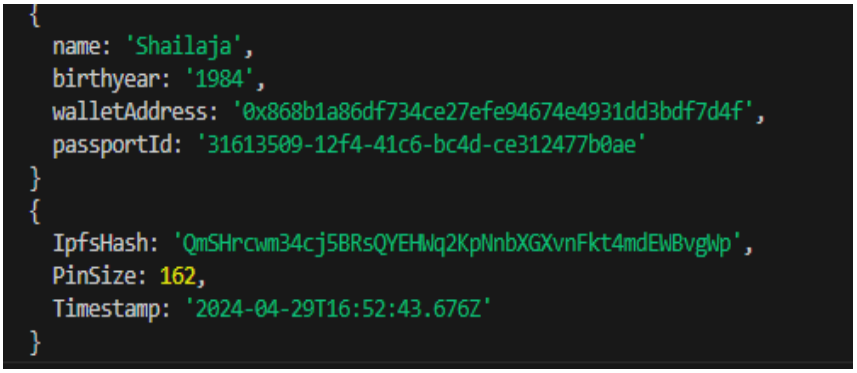

Fig.7. IPFS hash (CID) generated for user

The above screenshot shows the generation of unique id through IPFS which is bound with the Holder's wallet address for further generation of DID.

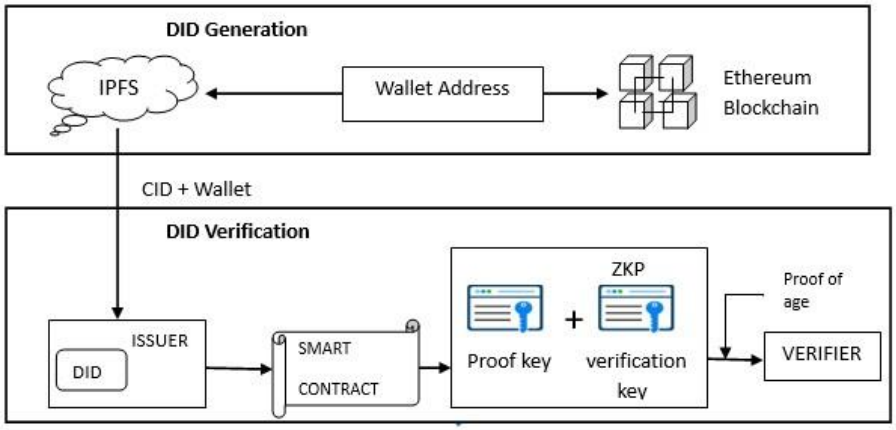

Fig.8. Architecture of the Proposed System

6. Selective Disclosure

Algorithm (3) : Verifier
Input: DID of user
Output: Verification Status

Step 1: Input the generated DID
Step 2: If an address is linked with the DID, then goto:ZKP alogirthm
Step 3: Else display message “DID does not exist”
Step 5: Stop

The Verifier algorithm plays a very important role in the complete ideneity management as, it is using the Zer- knowledge proof to verify tcertain details of an Identity holder, wtihtout revealing the Identification information.

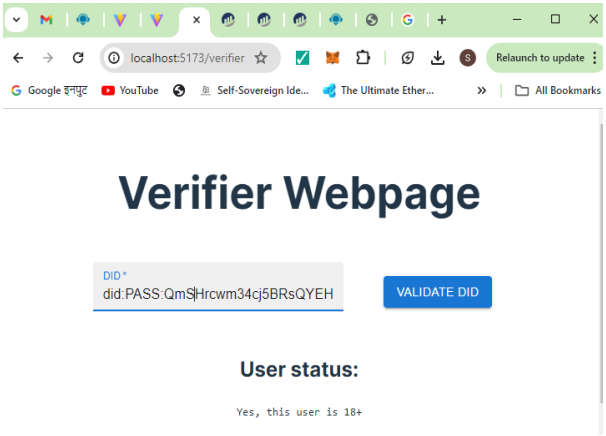

Fig.8. User status verified for age

Algorithm (4) : ZKP Algorithm
Input: DID of user
Output: Verification of age
Step 1: Extract the CID from DID
Step 2: Use CID to extract user data
Step 3: Extract “Birthyear” from retieved data
Step 4: Generated zokrates proof with keypair.pk and keypai.vk
Step 5: If (currectyear-birthyear)>= 18
Return “User is 18+”
Else
Return “User is under 18”
Step 6: Stop

The ZKP algorithm as explained in the terminologies sections plays a pivotal role in maintaining the authenticity of the identity, by being verifiable and at the same time, keeping the identity’s integrity.
The keypair : verifier key and proof key will generate the Zokrates verification key. The generated proof is in complete hashed format, un-readable by any user, system. This will give proof to the verifier by decoding the hashed proof with the keypair, which is otherwise difficult to intercept.

7. GDPR Compliance

The European Union(EU) ‘s GDPR (General Data Regulation Protection Regulation) regulatory principles [20], apply for anyone involved in processing personal data.As per the 5th Article’s 3.3 principle of GDPR, Data Minimisation ensures that the processed data is limited and only relevant information is used for the required purpose, since we have used the Zero-Knowledge proof zk-SNARK in the proposed method, the complete information related to identity of user is not revealed to the verifier, thus achieving the compliance. The principle. As per the 3.7 principle of Accountability, the other roles in Identity management are also satisfied,

as the proposed system uses a public blockchain, instead of a private blockchain, where the data handling can become difficult, thus the compliance with this principle can be stated.

8. Experimental Setup

The process of user Identity verification and authentication on digital platform can be affected by major constraints like network latency, delay. Our proposed system has taken into consideration these factors. The graph in Figure 9, shows the time taken for Issuer to complete the issuing of did to the holder and also the Registration of Holder with the attributes (Name, Birthyear). The time is in millis seconds, as per the network analysis, the total time from starting connection with IPFS server and creating the hash of id is 456.59ms and that of registration is 256.3ms.The graph in Figure 10, shows the times taken for Holder connection with the Ethereum wallet through Metamask, which is total 38.68ms, whereas, it is 64.49ms for issuing the credential. The testnet used for this implementation was sepolia network. The analysis, proves that Issuing credentials and generation of de-centralized identifier “DID” for a user can be achieved in a optimized amount of time, considering the gas fees and generation of hashes in the blockchain.

The proposed system efficiently utilizes the Blockchain ecosystem in conjunction with IPFS for easier and faster unipue Identity generation. As mentioned in the Related work, the emphasis on using Blockchain for achieveing SSI-based Identity Management system is achieved. The following table summarizes the principles of SSI achieved through the implementation.

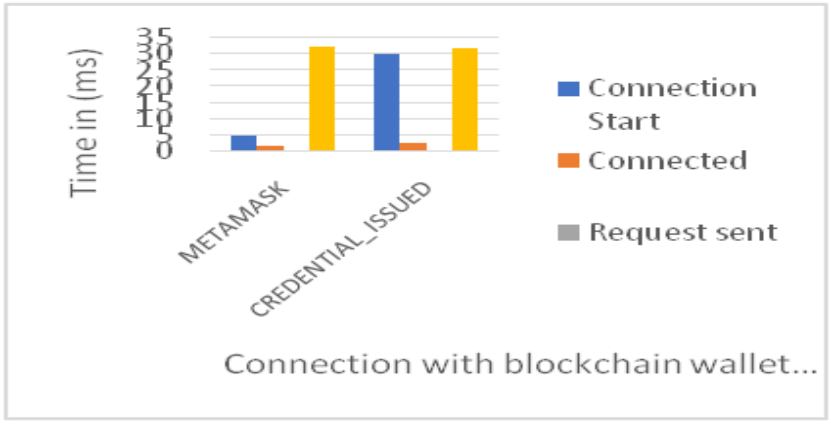

Fig.9. Time required for wallet and credetntial issuance

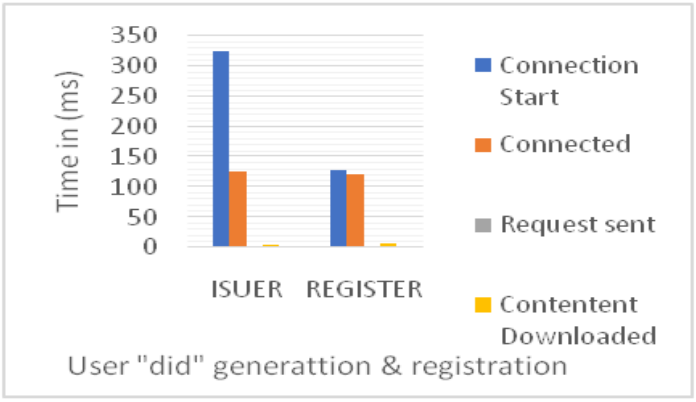

Fig. 10. Time required for DID generation

The system gives a SSI-based solution for Identity Issuance and Verification.

9. Results and Discussion

The system, inclusive of creating a unique de-centralized Identifier and Verification, gives a notion of de-centralized Identity Management. The encryption of DID during verification using zokrates library, allows the Identity a limited exposure, by hiding the underlying details like birth date of user. This makes the system more

secure and threat immune, the table below is a summary of the SSI principles, supported by this proposed system.

Table 1. SSI Principles supported by the system

SSI Principle	Feature	Supporting component
Control	Holder can create and maintain his identity related information, like in the case of our system, the Name and Birthyear in his wallet	Ethereum Wallet
Access	User can access their Identity from their connected wallets, without dependency on Issuer.	Ethereum Wallet
Persistance	did, once generated for specific user is constant throughout and stored and encrypted	IPFS and ZKP
Minimzation	Birth date need not be disclosed for age verification	ZKP (Selective Disclosure)

To evaluate the supported principles of SSI, a structured mathematical model is presented below, which helps is evaluating the Compliance of the said principles.

The model is presented in 3 parts:

1: Define the principles in Mathematical terms

2: Aggregate the Metrics for overall evaluation

3: Combined Compliance Score.

1.Define the Principles in mathematical terms

Property – Access

Variables : A_u - Binary variable indicating if user has access to their identity data (1 if true, 0 if false)

P_u – Set of permissions granted to user u

Model:

$Au = \{1 \text{ if } u \in P\ u$

0 otherwise

Property – Persistence

Variables: Tu – Total time duration, the user u's data has been available

T_{total} – Total time period considered

Model:

$Ppersist,u = \frac{Tu}{Ttotal}$

Property – Control

Variables : $C_{u,i}$– Binary variables indicating if user u controls the access of entity I (1 if true, 0 otherwise)

$R_{u,i}$ – Set of access rights for entity i controlled by user u.

Model:

$C_{u,i} = \{ 1 \text{ if } i \in R_{u,i}$

0 otherwise

Property – Minimization

Variables: D u, i- Amount of data shared by user u with entity i.

$D_{min,u,i}$- Minimum required data to be shared by user u with entity i.

Model:

$M_{u,i} = \{ 1 \text{ if } D\ u, i \leq Dmin,u,i$

0 otherwise

2. Aggregate the metrics for Overall evaluation

Access Compliance:

$A = \frac{\sum uAu}{|U|}$

Where |U| is total number of users

Persistence Compliance

$P\ persist = \frac{\sum uPpersist,u}{|U|}$

Control Compliance

$C = |U| \cdot |I|$

$C = \frac{\Sigma u \Sigma i\ \Sigma C\ u,i}{|U|.|I|}$

Where | I | is total number of Identity Context (one is considered in the proposed system)

Minimization Compliance:

$M = \frac{\Sigma u \Sigma i\ \Sigma M\ u,i}{|U|.|I|}$

3. Combined compliance score:

Compliance = α · A + β · Ppersist + γ · C + δ ·M

Where α, β, γ, δ are weights that sum at 1. (α, β, γ, δ=1)

Applying the Compliance score for the proposed system

Number of users = 3

Number of entities = 1

Access: A1=1, A2=0, A3=0

$A = \frac{1+0+1}{3} = \frac{1}{3}$ ------ *1*

P persist,1 = 0.9, P persist,2 = 0.8, P persist,3 = 1.0 -----*(Assuming the time duration of active connection with the wallet)*

$P\ persist = \frac{0.9 + 0.8 + 1.0}{3} = 0.9$ ----- *2*

Control: $C_{1,1} = 1, C_{2,1} = 1, C_{3,1} = 1$

$C = \frac{1 + 1 + 1}{3} = 1$ ----- *3*

Minimization: $M_{1,1} = 1, M_{2,1} = 1, M_{3,1} = 1$

$M = \frac{1 + 1 + 1}{3} = 1$ ----- *4*

Compliance =

$\frac{1}{4}\left(\frac{1}{3} + 0.9 + 1 + 1\right) = 0.80$ ---- *5*

From eq. 1,2,3,4 and 5 Compliance with achieved SSI principles in proposed system is 80%

10. Conclusion

The proposed system effectively shows the use of Ethereum blockchain, IPFS and zero-knowledge proof for Digital Identity Management using SSI principles. The Security, Portability and Controllability aspects of SSI are achieved through the approach. The zk_SNARK proof method is successfully implemented for verifying the user age and presenting the proof, which is encrypted to the Verifier, thus achieving the controlled access of Identification and giving user the control of his identity. The results also show the estimated time for the complete Registration, Authentication and Verification process, which is optimized in spite of use of Ethereum blockchain and the related transactions on Blockchain network. The achieved SSI principles are based on multiple users, single Identity Context. Future work would emphasize on multiple users as well as multiple Identity contexts.

References

[1] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, ``A quanti_abletrust model for blockchain-based identity management," in Proc. IEEEInt. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData), Jul. 2018, pp. 1475_1482.

[2] T. Hamer, K. Taylor, K. S. Ng, and A. Tiu, ``Private digital identity onblock chain," in Proc. CEUR Workshop, vol. 2599, 2019, pp. 1_7.

[3] J.-H. Lee, ``BIDaaS: Blockchain based ID as a service," IEEE Access,vol. 6, pp. 2274_2278, 2017.

[4] Y. Ren, F. Zhu, J. Qi, J.Wang, and A. K. Sangaiah, ``Identity management and access control based on blockchain under edge computing for theindustrial Internet of Things," *Appl. Sci.*, vol. 9, no. 10, pp. 1_16, 2019.

[5] Odelu, Vanga. "IMBUA: Identity Management on Blockchain for Biometrics-Based User Authentication." International Congress on Blockchain and Applications (2019).

[6] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, ``An identity management and authentication scheme based on redactable blockchainfor mobile networks," IEEE Trans. Veh. Technol., vol. 69, no. 6,pp. 6688_6698, Jun. 2020.

[7] C.-T. Tseng and S. S. C. Shang, ``Exploring the sustainability of the intermediary role in blockchain," Sustainability, vol. 13, no. 4, p. 1936,Feb. 2021

[8] R. Soltani, U. Trang Nguyen, and A. An, ``A new approach to client on boarding using self-sovereign identity and distributed ledger," in Proc.IEEE Int. Conf. InternetThings (iThings), IEEE Green Comput. Commun.(GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE SmartData (SmartData), Jul. 2018, pp. 1129_1136.

[9] Shailaja Nitin Lohar, Sachin Dilip Babar, & Parikshit Narendra Mahalle. (2021). A proposed approach for Digital Identity management using Self Sovereign Identity. International Journal of Next-Generation Computing, 12(2), 158–168. https://doi.org/10.47164/ijngc.v12i2.198

[10] Allen, C.: The path to self-sovereign identity.URL:http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereignidentity.html (2023)

[11] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[12] Andrew Tobin and Drummond Reed. 2016. The inevitable rise of self-sovereign identity. The Sovrin Foundation 29, 2016 (2016)

[13] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. 2019. In search of self-sovereign identity leveraging blockchain technology. IEEE Access 7 (2019), 103059–103079.

[14] Jøsang, Audun and Simon Pope. "User Centric Identity Management." (2005).

[15] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala,and M. Avital, ``Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," Blockchain, Res. Appl., vol. 2, no. 2, Jun. 2021, Art. no. 100014.

[16] R. Soltani, U. Trang Nguyen, and A. An, ``A new approach to client onboarding using self-sovereign identity and distributed ledger," in Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (Smart Data), Jul. 2018, pp. 1129_1136

[17] https://www.w3.org/TR/2022/REC-did-core-20220719/

[18] Yuan Cao and Lin Yang, "A survey of Identity Management technology," 2010 IEEE International Conference on Information Theory and Information Security, Beijing, 2010, pp. 287-293, doi: 10.1109/ICITIS.2010.5689468.

[19] Anh, Luong & Park, Jong. (2023). Privacy-Preserving Identity Management System on Blockchain Using zk-SNARK. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3233828.

[20] Ico.org.uk. (2020) Guide to the general data protection regulation (GDPR). [Online]. Available: https://ico.org.uk/fororganisations/guide-to-data-protection-regulation-gdpr/principles/

[21] Barros, M.D., Schardong, F., &Cust'odio, R. (2022). Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass. ArXiv, abs/2202.09207.

[22] Singh Kalpana& Dib, Omar &Huyart, Clément & Toumi, Khalifa. (2020). A novel credential protocol for protecting personal attributes in blockchain R. Computers & Electrical Engineering. 83. 106586.

[23] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, andK. N. Qureshi, ``Health-ID: A blockchain-based decentralized identity management for remote healthcare," Healthcare, vol. 9, no. 6, p. 712,Jun. 2021.

[24] S. Wang, R. Pei, and Y. Zhang, ``EIDM: A Ethereum-based cloud user identity management protocol," IEEE Access, vol. 7,pp. 115281115291, 2019.

[25] K. O. Asamoah, H. Xia, S. Amofa, O. I. Amankona, K. Luo, Q. Xia,J. Gao, X. Du, and M. Guizani, ``Zero-chain: A blockchain-based identity for digital city operating system," IEEE Internet Things J., vol. 7, no. 10,pp. 1033610346, Oct. 2020.

[26] X. Yang and W. Li, ``A zero-knowledge-proof-based digital identity management scheme in blockchain," Comput. Secur., vol. 99, Dec. 2020,Art. no. 102050.

[27] S. Friebe, I. Sobik, and M. Zitterbart, `DecentID: Decentralized and privacy-preserving identity storage system using smart contracts," inProc. 17th IEEE Int. Conf. Trust, Security. Privacy Comput. Commun., 12thIEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), Aug. 2018,pp. 3742.