Identity and Privacy Preservation through ZKPs

Rajat Subhro Bose, Tabrez Mohammed, Yash Saini, Tanvi Gupta

Abstract— **Privacy on the web is a major issue in the digital landscape. With growing concerns about data privacy, users are growing more wary of how corporations use, store or sell their data to third party organizations. This has led to an increase in an effort to offload data monopoly and control from IT giants and approach digital navigation from a user friendly point of view. This paper discusses a unique approach to solving the issue of data privacy and control using blockchain based decentralized self sovereign user identity solutions and highlights the use of zero knowledge protocols to empower users to choose what credentials to reveal and how much to reveal, thus letting the user be in control of their digital identity. The paper also details out the general concept, the working of the minimum viable product developed on Ethereum Blockchain using Solidity, system design of the same and finally the further plans related to the work.**

Index Terms— **Aadhar, Blockchain, Circom, Circomlib, Credentials, Cryptographic, Decentralized, Ethereum, Groth16, Hardhat, Identity, Metamask, Privacy, Proof, ReactJS, Self-sovereign, Sepolia, Smart contract, SnarkJS, Solidity, Soulbound, Verifiable, Verifier, Verification, Web3, ZKP, zk-SNARKs, Zero Knowledge.**

I. INTRODUCTION

The protection of individual identification and privacy has grown in importance as we move towards a time of digital connectivity and data-driven decisions. The study explores decentralized self-sovereign identity (SSI) preservation approaches and highlights the urgent need for creative solutions to protect individual identities in a digital environment that is fundamentally interconnected. The emergence of online interactions has exposed flaws in the conventional centralized identity management systems, leading to the investigation of alternative paradigms. In response to these difficulties, a number of solutions have been developed, each aiming to redefine identity management and give people more control over their personal data. Among these, distributed ledger technologies, particularly blockchain, stand out because they promise to transfer control away from centralized organizations and toward individual users. Blockchain enables the construction of tamper-resistant, auditable, and immutable identity records using cryptographic processes, potentially delivering a paradigm shift in how identity is handled and authenticated.

The investigation of Zero Knowledge Proof (ZKP) protocols, which form the basis of the suggested identity preservation framework, is at the heart of this paper. ZKPs make it possible to verify data without revealing the actual data, preserving privacy while also building trust in transactions. The paper aims to present an innovative approach to secure identity management where users retain full control over their personal information and institutions can reliably verify identities without compromising sensitive data by leveraging ZKPs in the context of blockchain-based SSI systems.

The foundation of contemporary cryptographic methods, Zero Knowledge Proof (ZKP) protocols signal a paradigm shift in data privacy and security. These protocols allow a prover to establish the truth of a claim without disclosing any information other than the fact that the claim is true. In summary, ZKPs allow parties to interact in ways that foster trust while making sure that sensitive information is completely hidden. This characteristic has drawn a lot of interest, especially in the context of blockchain technology, where ZKPs are used to improve efficiency, security, and anonymity. The use of ZKPs offers a significant resolution to the dilemma of balancing identity verification with data privacy within the framework of decentralized self-sovereign identity (SSI) maintenance. The difficulty lies in enabling institutions to validate these identities without sacrificing user privacy as SSI systems work to give

This work was done partly in collaboration with Samsung Research and development center, Bangalore, India. This work is inspired by a research problem originally presented during the Samsung PRISM student program. The original problem is the intellectual property of Samsung. The authors acknowledge the intellectual stimulus provided by the program while confirming that the results and interpretations are original and independently developed. The authors have modified and extended the problem independently for academic research purposes.

people control over their digital identities. ZKPs offer a graceful solution by enabling users to reveal only the information required for verification, obviating the need to divulge all of their personal data. A web application has been created as a Minimum Viable Product (MVP) to demonstrate the practical application of ZKPs in the field of SSI, serving as an embodiment of the ideas mentioned in the paper. This application illustrates how users can protect their privacy by asserting their identity claims to organizations without disclosing any sensitive information. The MVP creates a secure and privacy-respecting basis where people may confidently declare their identity claims and institutions can confirm these claims with a high degree of assurance through the integration of ZKPs.

II. BACKGROUND KNOWLEDGE OF ZERO KNOWLEDGE PROOFS

The development of Zero Knowledge Proof (ZKP) protocols has been a game-changer in the effort to decentralize digital identification on the web. The incorporation of ZKPs into identity management systems presents a compelling paradigm change in a time when worries about data privacy and security have grown. This strategy reduces the hazards connected with centralized warehouses of sensitive data while simultaneously giving people more control over their personal information.

At its core, ZKP enables a prover to convince a verifier of the validity of a statement without disclosing any details about the statement itself. In the context of digital identity, this translates into the ability to prove certain attributes or claims without revealing the underlying data. This capability is particularly relevant for enhancing the concept of self-sovereign identity (SSI), where individuals maintain full authority over their identity information. The use of ZKPs in decentralizing digital identification on the internet offers a number of compelling benefits:

Using ZKPs, people can choose to share only the information required for a given transaction or engagement. Data reduction guarantees that no more information is given than is necessary, protecting user privacy.

ZKPs are in line with the SSI idea, in which people have direct control over their identity traits. Users are encouraged to take a user-centric approach to identity management by being able to cryptographically validate their identity claims without relying on centralized authority.

Sharing sensitive data is frequently required for verification in traditional digital identification systems. ZKPs make it possible to verify information without disclosing the actual data, improving privacy by design.

Centralized identification systems are susceptible to single points of failure and significant data breaches, which reduces the attack surface. By removing centralized identity information repositories, decentralizing identification through ZKPs minimizes the attack surface. The decentralized identity landscape can be made more interoperable by standardizing and implementing ZKPs across a range of platforms. This opens the door for secure and smooth communication between various services. By utilizing ZKPs, people are given more precise control over the information they disclose and when they share it. This empowerment promotes a change in the balance of power between customers and service providers.

ZKPs can theoretically be included into online apps to enable safe and private interactions. For instance, a user can demonstrate their eligibility in online age verification without disclosing their precise birth date. Users can prove they have a specific set of credentials throughout authentication operations without revealing those credentials.

ZKPs hold great promise for decentralizing digital identification, but there are still difficulties. These include the difficulty of putting ZKPs into practice, potential performance overhead, and the requirement for technology user education.

III. METHODOLOGY

In this section, we incise the proposed privacy-preserving identity verification system architecture which uses Zero-Knowledge-Protocol (ZKP) and Ethereum Blockchain Network.

A. Firstly, let define the entities involved:

- R1cs file (Rank 1 Constraint System): The R1cs file is a representation of a rank 1 constraint system, which defines the constraints and relationships within a zero-knowledge circuit. The Circomlib library uses this file to generate a proving key, verification key, and other necessary components for generating and verifying zero-knowledge proofs.

- Wasm file: The Wasm file is a compiled binary file in WebAssembly format. It contains the compiled code that represents the zero-knowledge circuit generated from the R1cs file. The Circomlib library uses this file for efficient and fast execution of the zero-knowledge circuit within a web browser or other compatible environments.

- Verification_key.json: The verification_key.json file contains the necessary information to verify a zero-knowledge proof. It includes cryptographic parameters, public keys, and other metadata required for the verification process. Circomlib utilizes this file to verify the proof.json file against the specified constraints and determine its validity.

- The Groth 16 protocol is a non-interactive zero-knowledge proof (NIZK) protocol that provides a powerful and efficient method for proving the correctness of computations while preserving privacy. It is s based on zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), which are succinct proofs of knowledge that provide both computational soundness and zero-knowledge properties. zk-SNARKs employ a combination of cryptographic primitives and mathematical techniques to enable efficient proof generation and verification.

- The Power of Tau15 (PoT15) is a key ceremony in the field of zero-knowledge proofs, specifically in the context of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). It is a collective computation process that generates a trusted setup for zk-SNARK systems. It ensures the integrity and security of the common reference string used in zero-knowledge proofs. By employing a trustless and distributed setup approach, the Power of Tau15 ceremony provides a crucial foundation for privacy-preserving technologies in various applications.

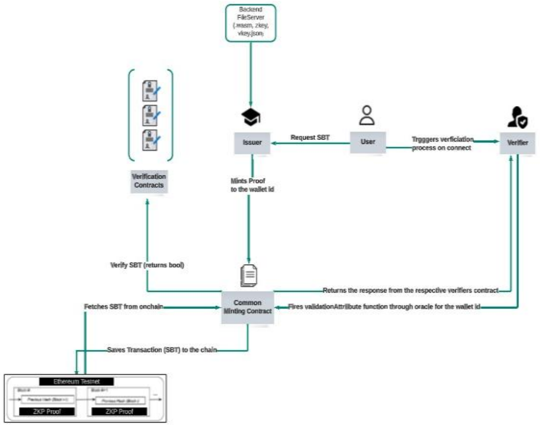

Backend FileServer (.wasm, zkey, vkey.json)
Verification Contracts
Issuer
Request SBT
User
Trgggers verficiation process on connect
Verifier
Mints Proof to the wallet id
Verify SBT (returns bool)
Common Minting Contract
Returns the response from the respective verifiers contract
Fetches SBT from onchain
Fires validationAttribute function through oracle for the wallet id
Saves Transaction (SBT) to the chain
Ethereum Testnet
ZKP Proof
ZKP Proof

Fig. 1. System Architecture

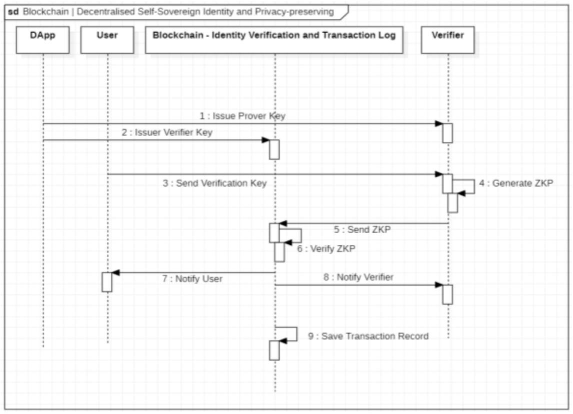

sd Blockchain | Decentralised Self-Sovereign Identity and Privacy-preserving
DApp
User
Blockchain - Identity Verification and Transaction Log
Verifier
1 : Issue Prover Key
2 : Issuer Verifier Key
3 : Send Verification Key
4 : Generate ZKP
5 : Send ZKP
6 : Verify ZKP
7 : Notify User
8 : Notify Verifier
9 : Save Transaction Record

Fig. 2. Abstract system workflow

B. Proposed workflow:

The Blockchain based Aadhar Card Identity verification system was designed and developed using Circom, SnarkJS, Hardhat, Metamask and Solidity. The smart contracts were deployed on Alchemy's Sepolia Testnet. Users can make use of the generate button to input their personal information and generate the proof. SnarkJS is used for the proof generation with the help of the files generated by the circomlib initially and served through a node js file server. On submission of valid data, the minting button is enabled through which one can mint the SBT after paying the gas fee for the transaction in the Sepolia Testnet. The proof is transformed into an object with keys a,b,c, and input before being minted. The frontend of the demo application was built using ReactJS and communications with the smart contracts are done through Wagmi. When a user enters the verifiers website and connects their wallet using metamask, the verification function is triggered and a response is displayed on screen. The architecture of the system is shown in Fig 1 and the description of the abstract workflow in Fig 2. Groth16 protocol is opted for in circomlib for a quicker process. A PoT15 key ceremony was undertaken for phase 2 contribution to make sure its integrity is not compromised. Circom was chosen for its beginner-friendly template and moderate abstraction which should allow the developers to also understand the underlying challenges and functioning of developing zk-circuits. The proposed system is able to ward off verification using fake identities. Unlike [4] our proposed system does not hold the uploaded information in any intermediary system making it also immune to eavesdropping. To give the verifiers the freedom to dynamically adjust the threshold values, we have developed the smart contract to accept variable public signals. The IVerifiers Interface in our common minting smart contract works like an oracle and calls the respective verfiers contract, eliminating the trouble of being connected with multiple smart contracts at once.

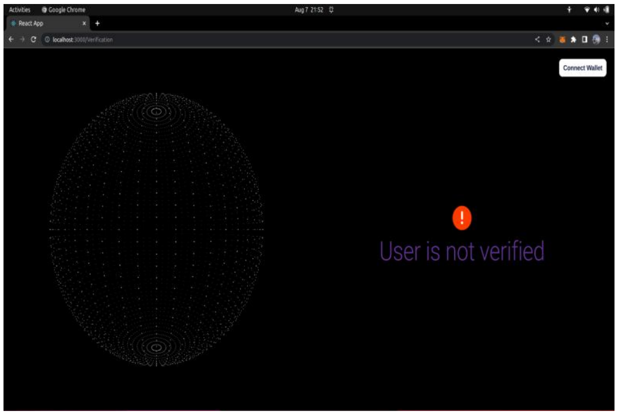
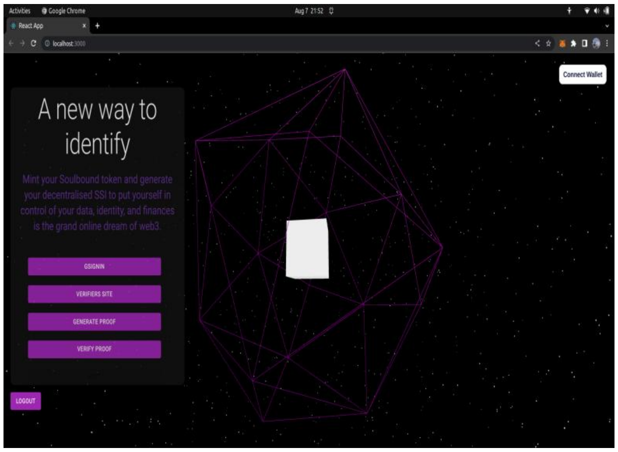

User is not verified

Fig. 3. Verifier page


A new way to identify

Mint your Soulbound token and generate your decentralised SSI to put yourself in control of your data, identity, and finances is the grand online dream of web3.

Fig. 4. Issuer page

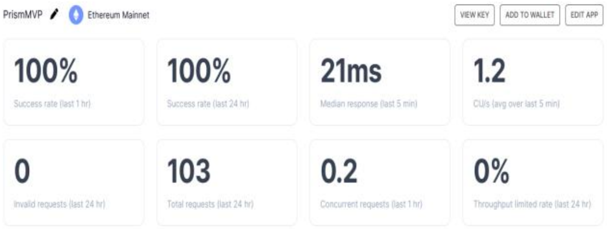
IV. RELATED WORK

In this section, novel works of other enthusiasts and professionals are outlined on blockchain in general as well as blockchain based identity verification systems. [9] provided the motivation to pursue a blockchain based identity verification system. The system proposed by them had a lesser negative impact on the environment while cutting the document verification time by huge margins. [1] constructed mobile application systems to emulate the obvious advantages of storing identities on blockchain with easy user onboarding in mind and thus, it advocates for a mobile application over a web app by drawing forth its survey analysis. [2] conceptualizes a EMC (European Mobility Card) using SSI principles to issue identity to all citizens with a fixed schema enabling them to be identified in public European public transports. Our idea is to create such a global identity linked to users mandatory documents to minimize the hassle in their lives while not compromising privacy. Unlike many other alternatives out there [3] also hold tamper proof consent receipt such a feature might encourage official entities to embrace SSI sooner. Concepts that compromise on a tad bit of privacy for better adoption rate are even more welcomed in the market like [4] in which uploaded are identities are exposed being stored in an intermediate system waiting to be issued by an admin. [6] uses SSI in a ride sharing app built on a permissioned chain using Hyperledger just like [7] but [7] lets the entities retain their legacy databases while adding a secure identity layer on top. Hyperledger offers a lot of solutions such as Aries and Indy which are considered the standard in the world of SSI. Permissioned blockchains offer more security and privacy but can only be effectively implemented in applications made for specific domains and use cases. [6] also has enhanced succinctness and high transaction throughput and does the verification in milliseconds. While looking for similar niche implementations, [10] was found to have adopted SSI in a healthcare system and seemed to have achieved increased patient control, less maintenance and lower risks. Such implementations provide reasons to consider using Blockchain in other domains too.

V. EXPERIMENTS AND EVALUATION

A. Experimental Setup and Performance Evaluation

The prototype of the proposed identity verification system consists of two primary portions. the ZKP module and the blockchain network. The ZKP module is programmed by using the Circomlib and SnarkJS. The blockchain network is developed on Ethernet. We instantiated multiple clients, generated proof and minted SBT to their account in the Sepolia blockchain network with chain-id, 11155111. The file server and website are run locally for the demo on Ubuntu 18.04 operating system with 2.8 GHz Intel i5-8400 processor and 16GB DDR4 memory. The median response time is about 20 milliseconds for the common minting smart contract through which all the verification requests are relayed.



100%
Success rate (last 1 hr)

100%
Success rate (last 24 hr)

21ms
Median response (last 5 min)

1.2
CU/s (avg over last 5 min)

0
Invalid requests (last 24 hr)

103
Total requests (last 24 hr)

0.2
Concurrent requests (last 1 hr)

0%
Throughput limited rate (last 24 hr)

Fig. 5. Performance of the deployed smart contract

B. ZKP Module:

In our experiments, the mean time for verifying a user is about 25 seconds. The solidity smart contract generated using SnarkJS is notably better than the other experiments done using the frameworks provided by Hyperledger Aries and Ursa. The template used to check the constraints of the input:

Algorithm 1 ZKP template

```
template IdentityCheck(){
signal input age;
signal input citizenship;
signal input cibil;
signal ageCheck;
signal cibilCheck;
signal citizenshipCheck;
signal interCheck;

signal output isSatisfied;

component greaterThan = GreaterEqThan(7);
greaterThan.in[0] <== age;
greaterThan.in[1] <== 18;
ageCheck <== greaterThan.out;

component equal = IsEqual();
equal.in[0] <== citizenship;
equal.in[1] <== 91;
citizenshipCheck <== equal.out;

component greaterThan2 = GreaterEqThan(7);
greaterThan2.in[0] <== cibil;
greaterThan2.in[1] <== 100;
cibilCheck <== greaterThan2.out;

interCheck <== cibilCheck * citizenshipCheck;
isSatisfied <== interCheck * ageCheck;
}

component main = IdentityCheck();
```

The above command is used to transform the circom template into the necessary files for proof verification and generation, later the generated proof generation files are served through the node backend while the verification smart contract is deployed on a Blockchain and its address is shared with the clients.

VI. CONCLUSION

By distributing identity verification processes across a network of nodes and employing cryptographic techniques, decentralized systems have the capacity to mitigate single points of failure and reduce susceptibility to large-scale data breaches. Developing standardized protocols, establishing clear legal frameworks, and building user-friendly interfaces will be pivotal in realizing the full potential of decentralized user identity systems. Ultimately, the pursuit of this innovative approach holds the promise of reshaping the digital identity landscape, empowering individuals with greater agency over their personal information in an increasingly interconnected world.

ACKNOWLEDGMENT

I would like to extend my gratitude to my peers, especially Tabrez Muhammad, Yash Saini and Tanvi Gupta who provided vital support for the research work and all those who supported me along the way. Their encouragement and assistance were essential in making this project a reality. I would also like to thank

Samsung Research and development center, Bangalore, India, for providing the opportunity to work on this problem.

REFERENCE

[1] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah and M. -A. Fatima, "Blockchain-Based Identity Verification System," 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2019, pp. 253-257, doi: 10.1109/ICSEngT.2019.8906403.

[2] Lukas Stockburger, Georgios Kokosioulis, Alivelu Mukkamala, Raghava Rao Mukkamala, Michel Avital, Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation, Blockchain: Research and Applications, Volume 2, Issue 2, 2021, 100014, ISSN 2096-7209. https://doi.org/10.1016/j.bcra.2021.100014. (https://www.sciencedirect.com/science/article/pii/S2096720921000099).

[3] Aydar, Mehmet, Serkan Ayvaz, and Salih Cemil Cetin. "Towards a Blockchain based digital identity verification, record attestation and record sharing system." *arXiv preprint arXiv:1906.09791* (2019).

[4] Devi, Sulochana and Kotian, Shrineeth and Kumavat, Manish and Patel, Dixit, Digital Identity Management System Using Blockchain (April 3, 2022). Available at SSRN: https://ssrn.com/abstract=4127356 or http://dx.doi.org/10.2139/ssrn.4127356.

[5] Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R. *et al.* Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. *EURASIP J. on Info. Security* 2021, 7 (2021). https://doi.org/10.1186/s13635-021-00122-5.

[6] W. Li, C. Meese, H. Guo and M. Nejad, "Blockchain-Enabled Identity Verification for Safe Ridesharing Leveraging Zero-Knowledge Proof," *2020 3rd International Conference on Hot Information-Centric Networking (HotICN)*, Hefei, China, 2020, pp. 18-24, doi: 10.1109/HotICN50779.2020.9350858.

[7] Guggenberger, T., Kühne, D., Schlatt, V. *et al.* Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes. *Electron Markets* 33, 3 (2023). https://doi.org/10.1007/s12525-023-00620-z.

[8] Feulner, S., Sedlmeir, J., Schlatt, V. *et al.* Exploring the use of self-sovereign identity for event ticketing systems. *Electron Markets* 32, 1759–1777 (2022). https://doi.org/10.1007/s12525-022-00573-9.

[9] G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899569.

[10] Mohammed Shuaib, Shadab Alam, Mohammad Shabbir Alam, Mohammad Shahnawaz Nasir, Self-sovereign identity for healthcare using blockchain, Materials Today: Proceedings, Volume 81, Part 2, 2023, Pages 203-207, ISSN 2214-7853, https://doi.org/10.1016/j.matpr.2021.03.083. (https://www.sciencedirect.com/science/article/pii/S2214785321021027)

[11] Ishmaev, G. Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics Inf Technol* 23, 239–252 (2021). https://doi.org/10.1007/s10676-020-09563-x

[12] Dr. Thanga Revathi, Dr.A.Gayathri, Dr.A.Sathya. Decentralized E-Voting and Governance System Using Blockchain. https://www.jisem-journal.com/index.php/journal/article/download/201/43/333