IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 27-29

Decentralized Way Of Identity Management Using Blockchain Technology

Siddhesh More[1], Kaustubh Nehete[2], Aditya Manjrekar[3], Amruta Pokhare[4]
[1]*(Information Technology, Atharva College of Engineering, India)*
[2]*(Information Technology, Atharva College of Engineering, India)*
[3]*(Information Technology, Atharva College of Engineering, India)*
[4]*(Information Technology, Atharva College of Engineering, India)*

Abstract : *Digital identity is one of the important aspect of digital economy. However, proving one's identity remotely is not that much easy. Centralized models of Identity Management are currently facing various challenges due to increasing number of data breaches which is causing loss of users data and privacy. Use of Blockchain Technology can help us to solve these issues. Blockchain Technology has revolutionized the entire mechanism of storing and maintaining the digital identity online. Also it helps to use digital identity globally as a legal identity proof or document. The main objective of this research is to find out solutions for current centralized identity management systems by the help of Blockchain Technology. The paper also includes a study of currently used systems for a better understanding of the technology.*

Keywords : *Blockchain Technology, Ethereum, Identity Management, IPFS, PKI.*

This paper proposes a way of digital identity management for individual users using the security of blockchain technology. Decentralization is a unique feature of blockchain. The sections of introducing blockchain for managing digital identity, its objectives, existing systems, proposed system, comparison with other systems are covered in this paper.

I. Introduction

Digital identity management system is the system that associates individuals with their respective online identities. It consists of issuing and maintaining IDs and certificates with respective information systems and providing the infrastructure that enables the verification of online transactions. The information contained in a digital identity allows authentication of a user on the internet without the involvement of human operators.

Individuals and organizations are often not in control over their own identities. Personal information is regularly shared across various online platforms and are prone to cyber-attacks. This paper demonstrates the various block-chain based solutions for digital identity management and proposes the approach to achieve the efficient management of identities.

II. Objectives

We have proposed a system with following aims:

• To build an application that creates decentralized digital identities.

• To develop a web application interface that accepts input identity data from the user which is then stored on the blockchain in a decentralized way.

• To review current industry practices and researches in regards to storing digital identities securely.

The result of this study will be valuable to the users who are looking to store their private information securely and have a complete control over their data.

III. Problem Statement

In today's scenario, we do not have a standard way to verify digital credentials and this is the reason because of which we are unable to use digital equivalent of any identity documents like driving license or birth certificate and we need to set up different usernames and passwords for various online domains for various activities. In the proposed system, we will be creating a distributed network of block-chain to store our identity documents. This system will accept file containing identity document as an input and will encrypt it and store it on distributed file system and hash of that file will be stored on the block-chain making it immutable. When another user will want to access that file, it only need to verify that hash and then have to decrypt it to get the original document.

IV. Existing systems

Current solutions for digital identity management are centered on public key infrastructure (PKI). Various issues of trust are associated with traditional PKI since it relies on centralized certificate authorities. This leads to single point of failure in PKI because certificate authorities are prone it being confused, hacked, mislead and bribed. Also, the user's information can get leaked due to systemic security risks in such centralized management systems. For example, aadhaar's data is stored on a centralized database which is accessed through a portal. This centralized system is vulnerable to attacks which may cause data leakage.

In federated identity management, users can use identity information that is established in one security domain to access another. This method is used by single sign-on schemes such as Facebook connect. Facebook has access to user's profile data whether it being public or private. It allows users to choose which data will be shared by Facebook with the relying party.

V. Proposed System

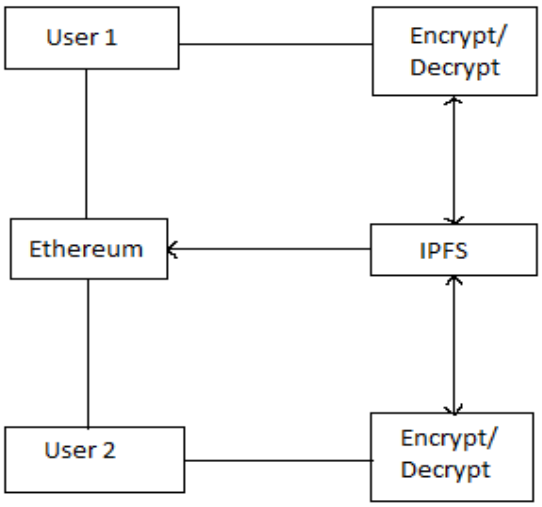

Fig.1 block diagram for the proposed system

The proposed system will be consisting of two important components as shown in above block diagram in figure 1. The first is IPFS which is distributed file system and second is Ethereum which is an open-source platform to build and deploy decentralized applications.

In the proposed system, file will be taken as an input from the user and it is encrypted using private key. Then it will be send to IPFS network to get stored. IPFS will return hash of the file. When another user wants that file, he can access it using hash of the file shared by the owner of the file. Then he will decrypt it using the public key of the owner to get the original file.

VI. Comparison With Existing Systems

The system thus proposed is different from the current existing systems in many ways which are as follows. The existing systems are mostly using centralized databases to store the users data. Also in federated identity systems, the data in existing domain is also stored in centralized databases only. So, if any failure occurs in central data repository then it will also affect the system [1].

Also existing systems should be trustworthy to make sure no information is being tampered. In the proposed system, we will be using a different approach where data will be stored in a decentralized fashion. In this, system will accept identity document file as an input and then encrypt it and store this encrypted file on IPFS. The hash of file returned by the IPFS will then be stored on Ethereum blockchain. Since we are not storing entire document, it will save cost. Also, because it is a decentralized system, it is more secure than the existing systems. So, it can be used as a valid identity proof for a user globally.

VII. Conclusion

The research helps to establish a digital identity management system to manage digital identities on the blockchain in a decentralized fashion. The system also provides a different approach than the systems that were used previously. This system uses web application to allow users to interact with the blockchain. It allows them

to store and share proofs of their personal information. This system will thus help in maintaining digital identities more securely.

References

[1]. C. Ellison; B. Schneier, A *"Ten risks of pki: What you're not being told about public key infrastructure,"* ComputSecurJ, *vol 16, no.1, pp, 1-7,2000*
[2]. Makoto Takemiya, Bohdan Vanieiev IEEE *2018 Sora Identity: Secure, Digital Identity on the Blockchain*
[3]. S. Nakamoto, Bitcoin: *A peer-to-peer electronic cash system, 2008*
[4]. D. Baars, *"Towards self-sovereign identity using blockchain technology,"* University of Twente, *2016*
[5]. IBM, *"Blockchain Technology for Recordkeeping"*, https://x9.org/wpcontent/uploads/2016/02/Blockchain-Explained-v2.09.pdf