Identity Management System Based on Blockchain Technology

Mohammad Shabib 19290116
Zaid Ibaisi 19290199
Mazen Houran 19290097

ABSTRACT

Identity is an integral part of a functioning society and economy. Having a proper way to identify ourselves and our possessions enables us to create thriving societies and global markets.
At its most basic level, identity is a collection of claims about a person, place, or thing. For people, this usually consists of first and last name, date of birth, nationality, and some form of a national identifier such as passport number, social security number (SSN), driving license, etc. These data points are issued by centralized entities (governments) and are stored in centralized databases (central government servers).
Existing identity management systems are neither secure nor reliable, In this study, we will propose a blockchain-based solution for identity management, to provide more privacy, security, and control over our identity documents.

I. INTRODUCTION

• Overview Of The Problem

Identity management systems consist of identifying, authenticating, and authorizing someone to access services or systems. An example of this would be a governmental ID card. Traditional identity management systems like paper-based IDs have several problems from being subject to loss, identity theft, and forgery. A more developed identity management system is a digital identity that increases the speed of processes by allowing for greater interoperability.

• Current System Challenges

The current system which is a composition of paper-based and digital identity possesses a lot of challenges,
identity loss, and theft, if the digital identity is stored centralized server, it becomes vulnerable to hacking. In 2021, there were 1,862 breaches, with nearly 294 million people impacted, with over 18.5 million records exposed [1].

Lack of control over personally identifiable information (PII), users don’t know where their PII has been stored nor how many times their PII has been shared without their consent [2].

People share their personal information online via different unknown sources or services that can put their identification documents into the wrong hands.

• Blockchain-Based Solution

A proper solution for the issues mentioned previously is using Blockchain Technology.

Blockchain solves identity theft and forgery by using digital watermarking -public-key cryptography.

Blockchain solves the issue of lack of privacy by using zero-knowledge Proofs and provides security that no third party can share or access users' PII without the users' consent, this can be achieved by using privacy-preserving techniques like cryptography, a verifying entity requesting a user to prove his/her name with a passport won't have access to the remaining information contained in the document (e.g. date of birth and place of birth).

Blockchain will eliminate the need for 3rd party KYC (Know Your Customer) organization since everything will be maintained in one decentralized ledger.

• Blockchain Benefits

To summarize the benefits of an identity management system blockchain-based system.

Decentralization, No personal identification documents of the users will be stored in a centralized server. All the documents that identify users get stored on their devices making them safe from mass data breaches. Also, there will be no single point of failure (SPOF), Therefore, SPOF ensures that the system will never be compromised [4].

Security, Blockchain will not store the actual user's PII directly, rather, it will store the hash of the data, which we will discuss in the Problem Formulation.

Consent, the system uses smart contracts to enable controlled data disclosure. Thus, data manipulation is not possible on the blockchain.

Universal ecosystem, Blockchain doesn't set any geographical boundaries. This means users can use the platform across borders to verify their identity.

Same Source Of Truth, Blockchain provides the same source of truth about which credentials are valid and who attested to the validity of the data inside the credential.

II. PROBLEM FORMULATION

In this section, we give a detailed definition of the problem and its security requirements.

Identity Management System. The system will be constructed on top of a permission blockchain network that meets the security requirements we address and overcome the technical challenges we specify.
There are five actors in the model of an Identity Management system: **identity owners**, **identity auditors**, **identity verifiers**, **registrar**, and a **platform** [3].

The identity Auditor, The auditor will check the PII provided by the user and will attest to the validity of The PII.
Auditors will have access to a government database that issued the documents, therefore they must be governmental employees, and they will make a transaction on the ledger indicating that this person’s documents have been verified which in return will increase the person’s **trust score** (explained below).

The identity owner can store their credentials in their personal identity wallet and use them later to prove statements about his/her identity to a third party (the verifier). Also, he could upload his/her PII documents to the platform.

A Credential is a set of multiple identity attributes and an identity attribute is a piece of information about an identity (a name, an age, a date of birth).

The registrar will be responsible for the registration of both the owners, verifiers and auditors.

The identity verifiers, the verifier is a 3rd party user who tries to check the correctness of the identity owner’s PII in a transaction.

A Platform, The platform will act as an environment to monitor the activities of the user, verifier, and auditor.

A platform is managed by a set of network players. Let’s briefly explain the reason with the following scenario: suppose there is a central authority -One Auditor- suppose there is some malicious identity auditor that tries to validate a false PII. In an ideal system, this behavior is expected to be easily detected. However, if the malicious auditor has enough power to control the central authority, they may keep this act without being detected and keep validating false PII for personal gain or agendas. Thus, to avoid such a scenario it will be better to **distribute** the control among a set of network players- multiple auditors.

A special mechanism will be used in this model, called the **trust score**. It’s used to measure the trustworthiness of an individual. The higher it is the more trustworthy a person is. The rules for this system are as follows; Validation of information such as name, phone number, address, Date of birth, etc. will increase your trust score adding more identification documents like passport, ID card, and a diploma will also increase your trust score. Moreover, making more transactions regularly will only result in increasing the trust score.

As for the rules that decrease the trust score, the changing of personal detail and profile more often will cause a decrease in your trust score. Also not using your ID actively will cause a decrease over time.

Security Model. We identify the security requirements for a decentralized identity management system.

Security Against a Malicious Identity Auditor. A malicious auditor may try to verify a PII without checking its validity of it. Security, in this case, will be achieved through assigning multiple auditors to each issued PII.

Security Against Malicious identity verifier. A malicious verifier may try to use users' PII for other reasons rather than verification (e.g selling users' PII). Security, in this case, be achieved by using Zero-Knowledge proofs. Zero-knowledge will enable the verifier to verify that the identity owner is what he/she claims to be without knowing the actual data.

Privacy Concerns, PII will be stored using hash functions the identity owner uploads the government-issued documents (passport, ID card, etc.) to the platform and these documents will be saved in the IPFS with hashed addresses stored in the blockchain.
InterPlanetary File System - IPFS: it's a decentralized, peer-to-peer file-sharing protocol. The IPFS network runs on the web and it's used to store data and retrieve it based on the file contents [5].

Since only the hashed addresses are stored on the blockchain the identity documents' content cannot be viewed on the blockchain by any user.

REFERENCES

[1] The Identity Theft Resource Center“ 16th Annual Data Breach Report” in idtheftcenter.org

[2] BLOCKCHAIN IDENTITY MANAGEMENT: ENABLING CONTROL OVER IDENTITY in leewayhertz.com

[3] Actors in Identity Management with Blockchain in tykn.tech

[4] Innovation Insight for Decentralized Identity and Verifiable Claims in gartner.com

[5] InterPlanetary File System in wikipedia.org

[6] Yang Liua, Debiao Hea, Mohammad S., Neeraj Kumarf , Muhammad Khurram Khang , Kim-Kwang Raymond Chooh “Blockchain-Based Identity Management Systems: A Review” in sciencedirect.com