BBM443
FUNDAMENTALS OF BLOCKCHAIN

DIGITAL IDENTITY BASED ON BLOCKCHAIN TECHNOLOGY

17.12.2021

GROUP 8
21827555 - Meltem KAYA
21827349 - Beyza ERDOĞAN
21828035 - Selçuk YILMAZ

Table of Contents

Introduction

In today's world, we know that our identity is the most valuable thing that we own. It is unique for everybody and distinguishes us from everyone else; it defines us. And in a world that keeps digitalizing, our identities will be affected by this digitalization inevitably. This evolution introduces us to a new concept: "Digital Identity". A **digital identity** is an online or networked identity adopted or claimed in cyberspace by an individual, organization, or electronic device. Since it includes valuable information like social security number, username, password, date of birth, we need to store and protect these securely against identity thefts and malignant sources. At that point, blockchain technology helps us - but how? In this paper, we will talk about digital identities, how blockchain helps implementing this concept and the problems that may arise.

State-of-the-Art

There is a lot of research for digital government systems. As an example, the Australian government supports and tries to implement digital identity for their system. Digital Identity System. It is a big step for our lives. Digital identity in government will accelerate our life with government issues that require identity verification.

Analysis

An identity document is any document that can be used to prove an individual's identity. It basically defines the person's uniqueness. The main challenges of traditional identity management methods can be grouped into four categories: Usability, Privacy, Security and Globalization.

Remembering lots of login credentials, having an excessive amount of login information for each service, and giving out private information for recovery of an account just in case of forgetting the password can cause a lot of burden to the user.

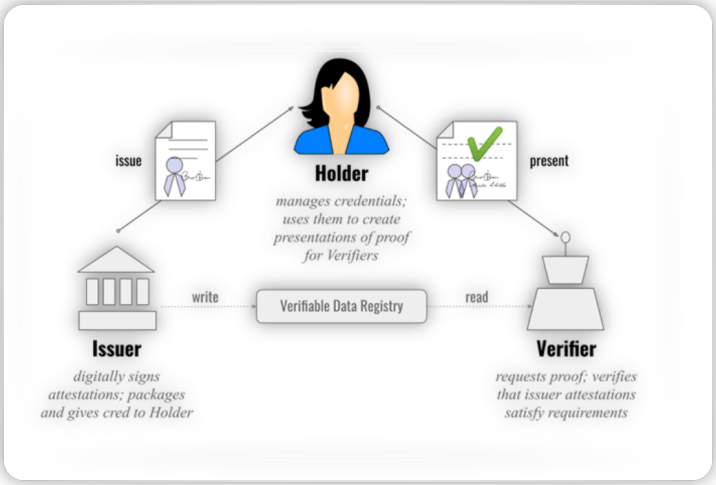
In traditional systems, an individual's identity assets are stored by third parties. And these include sensitive identity details that you wouldn't want to share with any other third party without your approval. Storing of these assets leads to privacy violation, since they are shared and exploited for commercial purposes without permission.

The vulnerability of many of the traditional systems software leaves an open door for hackers to steal identity information. In today's world, cyber-security breaches are increasing, and this also comes with a rise in economic damages. So, our identities are not securely protected and this is an important issue.

From a global perspective, identity verification and record attestation are challenging tasks across borders due to the institutional and international barriers. It costs a lot of money and time.

A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization, or device. It provides reliable authentication and enables delivery of a variety of services via web or mobile applications that require proof of identity.

The Trust Model



The main specifications that deal with digital identities place them within the framework of the trust model of the Issuer/Owner/Verifier relationship. This is usually depicted in a triangle and shows the flow of digital identity-related information between parties.

Figure 1. *Trust Model* **(Hancock, 2020)***

Proposed Model

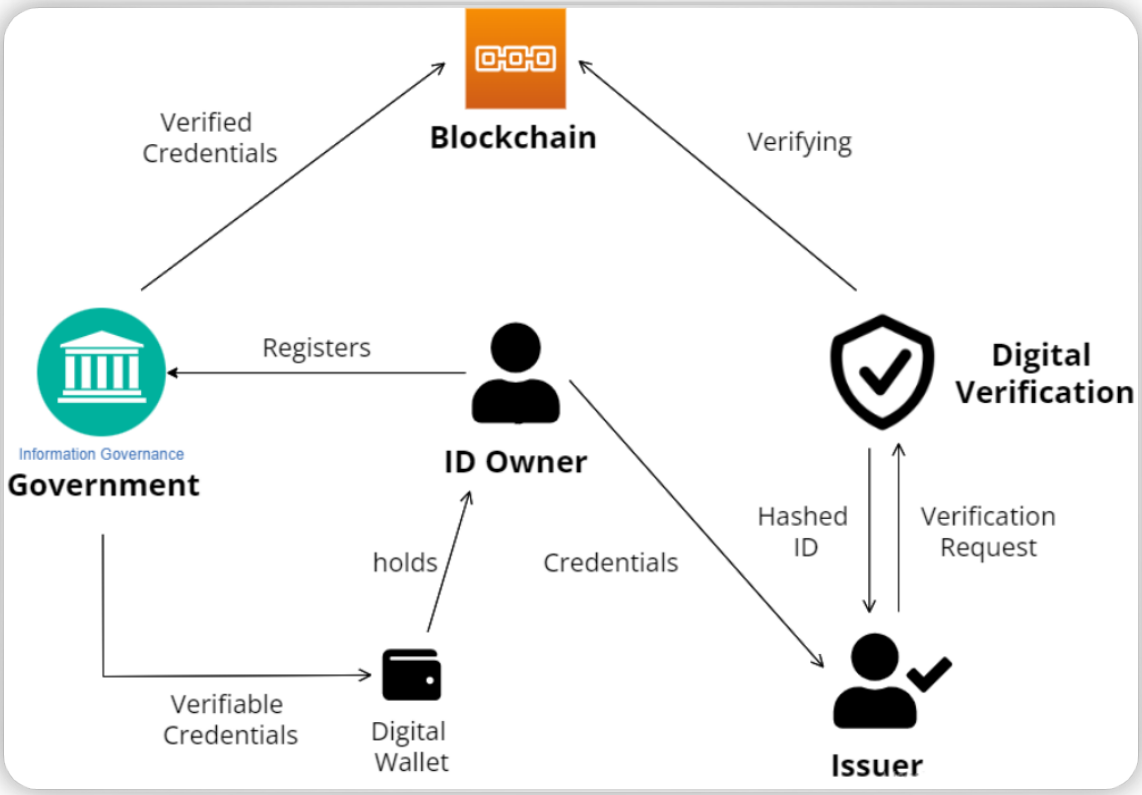


Figure 2. *Visualization of The Proposed Model*

In our model, the user's information is shared with the government when he/she registers. Then, the government stores the verified credentials to the blockchain. When the user shares his/her credentials with an issuer, the issuer sends a request to the blockchain for verification. If the information is validated, the issuer receives the hashed ID of the user.

Implementation Details

We aim to build our software on Ethereum. Because Ethereum is the optimal platform for the Proof of Authority proof system. In proof of authority users can see validators publicly. With that users can trust to get in the system.

Our aim is to use Proof of Authority for this project. In the Proof of Authority method, validators share their reputation on the network. Nodes that become validators are the only nodes

allowed to generate new blocks. Compromised authenticators are encouraged to secure and protect the blockchain network. Also, the number of validators is quite small. The authorization system has a high transaction rate. Because blocks are generated in a series at a time interval assigned by authorized network nodes. This increases the speed at which transactions are verified. This is important because there are millions of people and the system must run reliably and quickly. Proof of Authority does not require nodes to spend computational resources to solve complex mathematical tasks and this gives us high performance.

Aspects of Our Model

1 - Proof of Authority

Proof of Authority is a reputation-based consensus algorithm that offers a practical and efficient solution to blockchain networks. It relies on known and reputable validators to produce blocks, and thus, provide computational power to a network. (CoinMarketCap)*

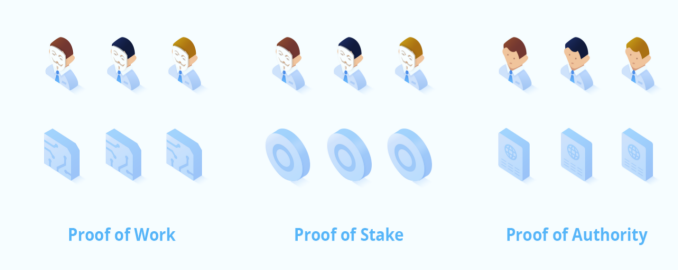
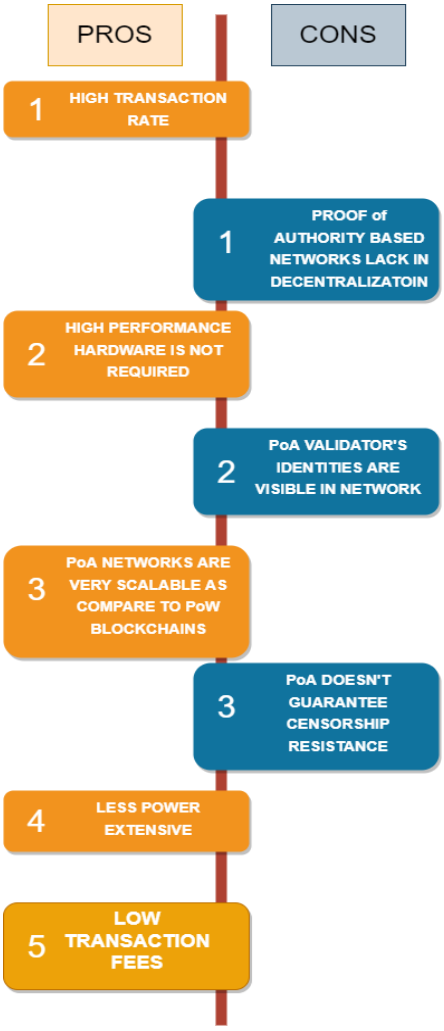


Figure 3. *Proposed Model* **(Poa Network, 2017)***

1.1- Why Do We Use POA?

Proof of Authority requires minimal computational effort and it doesn't need specialized equipment. It is best suited where there is some level of trust in the system. In that case, the government already has some level of trust so we can easily say that Proof of Authority is the best option. Also, validators must be reliable, so they can't be an ordinary person. PoA networks typically have a relatively small number of validating nodes, which makes them less decentralized.

Figure 4. *Pros vs. Cons of POA*



2 – Decentralized Architecture

Decentralized architecture enables data exchange where decentralized identifiers can be replaced with self-contained, independent identities and using blockchain and distributed ledger technology to protect privacy and secure transactions.

Figure 5. *Decentralized Architectures*

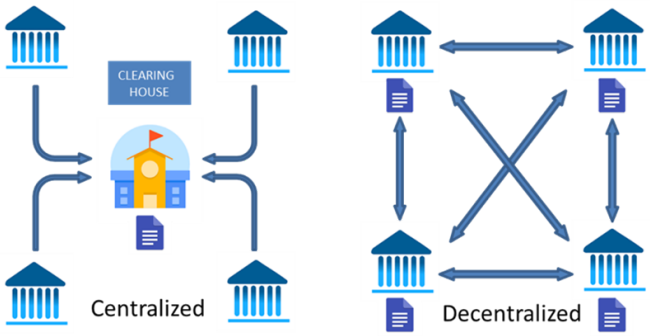
2.1-Benefits of Decentralized Architectures

- Provides a trustless environment

- Improves data reconciliation

- Reduces points of weakness

- Optimizes resource distribution



Weaknesses of Our Model

1. Using Proof of Authority on a decentralized system makes it less decentralized.
2. Although keeping personal data encrypted on the blockchain is safe for now, it may create a security vulnerability with the technological progress that may occur with quantum computers in the future.
3. Decentralized system has a few disadvantages like it is difficult to know which node failed, difficult to know which node responded, etc.

Results

Remembering lots of login credentials, having an excessive amount of login information for each service, and giving out private information for recovery of an account just in case of forgetting the password can cause a lot of hassle to the user. Therefore, traditional identities can be a burden for users when it comes to usability.

The use of civic identity evolves with digital identity. Originally used for physical checks, the ID is associated with a document that allows the owner to prove his identity by checking his photo. As the digital world evolves, identity tends to be used for new purposes, including the possibility of gaining access to online services or electronic services.

In today's digital age, we cannot do without a digital identity. Our digital identity is the version we have in the digital world. We need it so we can access almost everything in the digital realm, and we need it so that devices and their networks can accurately identify us so they can interact with us in a way that best suits our interests and preferences.

References

[1] Hancock, Alexis. (2020, August 31). *Digital identification must be designed for privacy and equity.*
https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

[2] CoinMarketCap. *Proof-of-authority (poa).*
https://coinmarketcap.com/alexandria/glossary/proof-of-auth

[3] Poa Network (2017, November 11). *Proof of authority: consensus model with identity at stake.* Medium.
https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

[4] Aws. *What is Decentralization? Benefits of decentralization*
https://aws.amazon.com/blockchain/decentralization-in-blockchain/