Blockchain Based Identity Management System

CS2DDA: Data Encryption, Data Integrity and Authentication

George Hotten (XXXXXX352)

December 13, 2024

Word Count: 1,365

Contents

1 Introduction

In this report, I will review and analyse the most effective networks, consensus mechanisms, and identity management models for creating a blockchain based identity management system. For this system, I have chosen to use a hybrid network, delegated proof of stake consensus mechanism and a self-sovereign identity management model. These choices were made to provide users with the most privacy whilst not comprising on security and transparency. They were also to ensure that the system is accessible to those with limited computational power.

2 Hybrid Blockchain

I have chosen to use a Hybrid Blockchain for my identity management system. Hybrid Blockchains use both public and private blockchains, allowing me to leverage the advantages of using both public and private blockchain technologies. (Naik, 2024*a*)

This type would give me full control over the privacy and the customizability of the system, for example I can control what data is made publicly available. (Naik, 2024*a*) It would also give me full control of what consensus mechanism to use and also the flexibility to change it in the future. (Itexus, 2024) The hybrid model would also allow me to utilise both the private and public sectors for both hash generation and verification (Naik, 2024*a*) and transparency: showing transaction details on a public ledger without exposing any sensitive information. (Itexus, 2024)

With Hybrid blockchains providing the best of both public and private models, Itexus (2024) describes the benefits of using this model:

- Enhanced Privacy and Security—you have full control of what information is shared whilst providing public verification records.
- Efficient and Scalable—different consensus mechanisms can be used on the private and public sides of the blockchain.
- Flexible Access Control—especially for an identity management system, a hybrid model allows for tailored requirements in privacy.
- Improved Compliance with Regulations—full flexibility to comply with GDPR for what data is publicly accessible.
- Enhanced Transparency—regulatory bodies and customers can have transparency for how data is processed.

3 Delegated Proof of Stake

For the consensus mechanism, I have chosen to use Delegated Proof of Stake. Delegated Proof of Stake (DPoS) is a model that utilises both stakeholder voting and democracy (Makovský, 2024). This allows blockchain participants to vote on delegates who create and validate the blocks in the network (Naik, 2024*a*).

This consensus mechanism would allow me to have much more control over ensuring that legitimate blocks are created and validated, as in the event of a malicious user, they can be voted out of the system. DPoS is also more efficient, allowing for shorter block production periods and higher transaction volumes (Saad and Radzi, 2020). With this efficiency, there is also lower computational requirements compared to mining related mechanism allowing for easier scaling within the network (Naik, 2024*a*).

Howell (2022) describes some of the advantages of using DPoS:

- Faster validation of transactions - the quicker the user is at processing, the more likely they'll be voted in.
- Energy efficiency - DPoS does not need as many resources as a mining related consensus mechanism.
- Democratic voting - every token holder has a way of contributing to and developing the network.
- Voting out - delegates can be voted out if malicious actions are suspected.
- Enchanced security - the ability to vote out malicious delegates enhances the overall security of the network.

4 Self-Sovereign Identity

For the identity management model I have chosen Self-Sovereign Identity. Self-Sovereign Identity (SSI) is a "user centric identity system" that gives users a direct link between themselves and the organisation, removing the need to use a third-party identity provider (Naik, 2024*b*). Naik (2024*b*) further describes how an identity is provided to the user by an 'issuer' who creates the credentials. When required, these credentials are given to the 'verifier' who validates their authenticity.

SSI utilises two new standards: Decentralized Identifier and Verifiable Credentials.

4.1 Decentralized Identifier

A Decentralized Identifier (DID) is a universally unique identifier that is permanently issued to a user, utilizing a URN that resolves to a DID document. The DID document often contains data such as public keys for verification, authentication methods, service endpoints, timestamps, and signatures (Naik, 2024*b*).

4.2 Verifiable Credentials

Naik (2024*b*) describes how Verifiable Credentials (VC) are a digital signature proving: who the issuer is, who the owner is, whether it has been modified, and whether it has been revoked. VCs also give the identity owner control over what data they share, such as the entire credential, part of the credential, or a zero-knowledge proof token from the credential.

4.3 Advantages of SSI

Okta (2024) describes the following advantages of SSI:

- Credential issuing is simple - making use of DID and VC.
- Credential verification - identities can be verified at any time, even if the issue no-longer exists.
- Encrypted credentials - the credentials cannot be tampered with.
- Decentralized system - giving users higher privacy and making it harder for an attacker to steal personal information.
- Privacy is under the user's control - the user dictates what information is published and what is kept private with the verifier.

5 Critical Analysis

To recap, I have chosen the following elements for the identity management system:

- Blockchain Network - Hybrid.
- Consensus Mechanism - Delegated Proof of Stake.
- Identity Management Model - Self-Sovereign Identity.

5.1 Blockchain Network Analysis

I have chosen the Hybrid model over the other models due to its unparalleled control over privacy and customizability. In a public blockchain, all data is accessible to anyone who participates, and private blockchains you must be admitted into the network to see any data at all. The private blockchain also is not completely decentralized (Naik, 2024*a*). This removes layers of transparency and makes them more susceptible to data breaches and security threats, which is also a direct cause of fewer people to validate and audit data within the network (Seth, 2024).

This makes Hybrid the perfect choice as it leverages good privacy through the private blockchains whilst also maintaining the transparency found on public networks. An example of this is shown by Itexus (2024) where transaction details can be found on a public ledger, whilst all private and confidential user data can be kept on the private ledger. The hybrid model further allows the system to adapt as its needs change, as it isn't restricted by a single model. Naik (2024*a*) also describes how using both public and private networks allows me to increase security by creating hashes on the private ledger and then verifying them on the public ledger.

5.2 Consensus Management Analysis

I have chosen the Delegated Proof of Stake (DPoS) consensus mechanism due to its use of stakeholder voting and democracy (Makovský, 2024), alongside its great efficiency and speed (Saad and Radzi, 2020). Comparing DPoS to Proof of Stake, PoS uses a pseudo-random election process rather than a democratic vote, which risks fraudulent blocks being validated by bad actors. The higher stake you have, the higher chance you will get selected to verify transactions. This is less superior to DPoS as it requires a fully democratic vote between stakeholders on which participants will validate new blocks. This also has better fraud protection, as if someone attempts to validate a fraudulent block, they can easily be removed and replaced by another delegate (Naik, 2024*a*).

Further compared to Proof of Work, DPoS is more efficient and quicker (Saad and Radzi, 2020) as PoW requires users to solve complicated mathematical puzzles which require a large amount of computational power and has high energy usage. This discourages people from contributing to PoW blockchains as the reward of solving the puzzles would have to outweigh the cost of components and electricity (Naik, 2024*a*).

5.3 Identity Management Model Analysis

I have chosen the Self-Sovereign Identity Management (SSI) model because of its universal and decentralized approach. Unlike Federated Identity Management and Centralised Identity Management, where user data is controlled by a third party, SSI allows for individuals to have full control over their identity and the related data (Naik, 2024*b*).

SSI uses a universal Decentralized Identifier, which contains Verifiable Credentials that allows the user to specify what data is shared with whom. It further provides security into ensuring the VC has not been tampered with and that it has not been revoked or expired by the issuer. All data found on a VC is encrypted, giving the user extra security and control of their data (Naik, 2024*b*).

References

Howell, J. (2022), ‘Delegated proof of stake (dpos) - explained’. Accessed: 13 December 2024.
URL: *https://101blockchains.com/delegated-proof-of-stake-dpos/*

Itexus (2024), ‘Hybrid blockchain: Bridging the best of public and private blockchains’. Accessed: 12 December 2024.
URL: *https://itexus.com/hybrid-blockchain-bridging-the-best-of-public-and-private-blockchains/*

Makovský, J. (2024), ‘How does delegated proof of stake (dpos) work and which projects use it’. Accessed: 13 December 2024.
URL: *https://tatum.io/blog/delegated-proof-of-stake-dpos*

Naik, N. (2024*a*), ‘Blockchains’. Lecture Notes on CS2DDA, Aston University.

Naik, N. (2024*b*), ‘Identity management and access control’. Lecture Notes on CS2DDA, Aston University.

Okta (2024), ‘Self-sovereign identity (ssi): Autonomous identity management’. Accessed: 13 December 2024.
URL: *https://www.okta.com/uk/identity-101/self-sovereign-identity/*

Saad, S. M. B. S. and Radzi, R. Z. R. M. (2020), ‘Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos)’, *Place of publication: ResearchGate.* pp. 27–29.

Seth, S. (2024), ‘Public, private, and permissioned blockchains compared’. Accessed: 13 December 2024.
URL: *https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/*