DSF Blog

DLT Science Foundation

Apr 07, 2023

CONTENTS

Check out the blog pages below.

- *Governance In DeFi*
- *Self-Sovereign Identity: Technical Foundations and Applications*
- *Mobile Theft Prevention using Blockchain*
- *References*

CHAPTER

ONE

GOVERNANCE IN DEFI

Key Insights

- The voting power in DeFi protocols becomes increasingly concentrated among a percentage of token holders over time in decentralised exchanges, lending protocols and yield aggregators.
- The paramount wallet addresses ranking within the top 5, 100, and 1000, exercise predominant influence over the voting power in the Balancer, Compound, Uniswap, and Yearn Finance protocols, with Compound displaying the least evidence of decentralisation.
- The most significant governance challenges identified by DeFi users are voter collusion, low participation rates, and voter apathy.
- To address vulnerabilities in DeFi governance, a novel voting mechanism resistant to sybil attacks called bond voting has been proposed.
- To enhance the manual parameter section, an AI-enabled adjustment solution has been demonstrated to automate governance mechanisms.

1.1 Introduction

Decentralised finance (DeFi) has emerged as a potential substitute for traditional financial institutions, offering peer-to-peer transactions and a diverse range of services that democratise finance by enabling users to participate in protocol governance. However, several studies have suggested that the current governance mechanisms require improvements. This article provides an overview of findings associated with DeFi governance.

1.2 Centralisation of Governance in DeFi Protocols

Lending Protocols

Lending Protocols are DeFi applications built on top of blockchain technology that allow users to lend and borrow cryptocurrency assets without the need for intermediaries such as banks or traditional financial institutions.

Decentralized Exchanges

Decentralized Exchanges (DeXs) are peer-to-peer trading platforms built on top of a blockchain that enable the direct exchange of cryptocurrency assets without the need for a central authority or intermediary.

Yield Aggregator

Yield Aggregator are DeFi applications that automate the process of seeking out the best yield opportunities for cryptocurrency assets, and provide users with a way to optimize their returns on investment.

Centralisation in DeFi has become a growing concern among researchers with several studies identifying a significant level of centrality in the governance mechanisms of DeFi protocol. Barbereau et al., [BSP+22a] found that the decentralisation of voting is significantly low with a majority of the voting power concentrated among a percentage of governance token holders. As evidenced by their findings, there was a significant degree of centrality, in lending protocols, decentralisd exchanges and yield aggregators. This research work employed case studies to comprehend the governance mechanisms of these protocols.

Similarly, result by Jensen et al. [JvWR21] demonstrate centrality in voting power with the protocols top 5, top 100, and top 1000 wallet addresses controlling majority of the voting power in Balancer, Compound, Uniswap and Yearn Finance protocols. In this study, the token holdings and users' wallets of protocols were analysed; Compound displayed the most evidence of centrality and Uniswap the least with the top 5 wallet addresses accounting for 42.1% and 12.05%, respectively.

Barbereau et al. [BSP+22b] ascertained that DeFi protocols become more centralised over time. In this longitudinal study, voting patterns demonstrated changes in the power dynamics as time progressed. The tendency for this centralisation of DeFi protocols is shown in [Fig. 1.1]. Furthermore, in analysing the governance structures of DeFi protocols, Stroponiati et al. [S+] ascribed reward-based economic incentives as the significant cause behind the development of centralised structures.

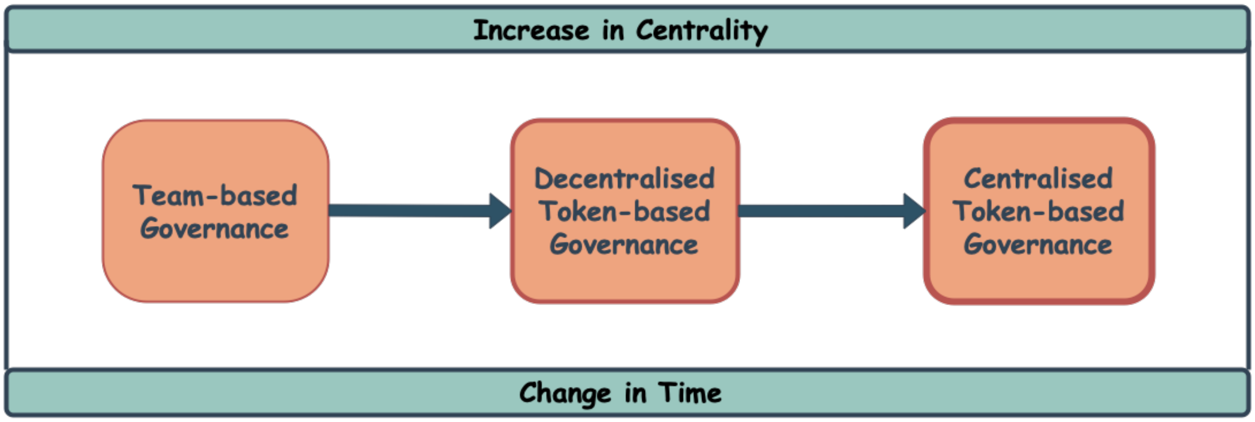
Increase in Centrality
Team-based Governance
Decentralised Token-based Governance
Centralised Token-based Governance
Change in Time

Fig. 1.1: The Tendency for Centralisation in DeFi Governance.

1.3 Challenges & Vulnerability In DeFi Governance

Voter Collusion

Voter Collusion refers to a situation where a group of voters collude together to manipulate the outcome of a voting process in their favor, typically by coordinating their votes to create a super majority.

Voter Apathy

Voter Apathy refers to a situation where token holders or members of the organisation do not actively participate in the voting process due to a lack of interest

In investigating governance challenges, Ekal et al., [EAw22] identified voter collusion, low participation rates, and voter apathy as the most significant challenges. This empirical investigation utilised an interview survey approach to collect data from protocol users. Furthermore, to address vulnerabilities, Mohan et al. [MKB22] proposed a novel voting mechanism resistant to sybil attacks called bond voting. This solution factors in time commitment to be resistant to plutocracy.

1.4 AI-enabled On-chain Governance

To enhance and automate governance mechanisms, Xu et al., [XPFL23] demonstrated an AI-enabled parameter adjustment solution which is more efficient than current implementations. Specifically, the study employed Deep Q-network (DQN) reinforcement learning to investigate for automated parameter selection in a DeFi environment. Although a lending protocol was employed in the study, the model's application can extend to other categories of DeFi protocols as well. In investigating DAOs, Nabben [Nab23] observes that GitcoinDAO also employs algorithmic governance in various organisational components such as monitoring the compliance with rules of the organisation.

1.5 Conclusion

The vision of DeFi is to forster a democratic process of governance and sustain high levels of decentralisation. However, recent studies have highlighted significant centrality in DeFi governance mechanisms, indicating the need for improvements in the existing governance models. The studies analysed in this article have revealed that the majority of the voting power in several protocols is concentrated among the top token holders, with evidence of increasing centralisation over time. Moreover, DeFi has been found to face challenges in the voting and governance process. In view of some of these challenges, researchers have proposed novel solutions such as a bond voting and a AI-enabled parameter-selection solution to improve the current mechanisms. Given the importance of decentralisation in the underlying philosophy of DeFi, proposing more solutions to governance challenges is crucial for creating a more inclusive and democratic financial ecosystem. Therefore, continued research and development will ensure be required.

CHAPTER

TWO

SELF-SOVEREIGN IDENTITY: TECHNICAL FOUNDATIONS AND APPLICATIONS

Key Insights

- SSI systems use DIDs as unique, resolvable identifiers for each entity, allowing the secure management of digital identities without relying on a centralised authority.
- VCs provide cryptographically verifiable proof of an individual's attributes or personal information, enabling secure and trustworthy data sharing between issuers, holders, and verifiers.
- SSI incorporates privacy-preserving mechanisms such as zero-knowledge proofs and selective disclosure, allowing users to prove their credentials without revealing their actual identity or unnecessary information.
- While not mandatory, using Blockchain as a decentralised data registry in SSI systems enables secure, tamper-evident, and verifiable storage of credentials, enhancing the trustworthiness and reliability of the identity management process.

2.1 Introduction

According to World Bank estimates, nearly 850 million people lack an official identity [JC23], and the proliferation of digital devices has made it increasingly essential to possess a verifiable digital identity. This has led to a rise in digital transactions and the need for a secure and reliable identity management system. SSI is emerging as a decentralised alternative to traditional centralised identity management systems, in which identities are cryptographically verifiable. It allows individuals to control their digital identities and share them with trusted parties. Each entity in the SSI system is identified by a unique DID (Decentralised Identifier) as shown below, which can be resolved to reveal information such as the entity's public key and other metadata.

$$\underbrace{\texttt{DID}}_{\texttt{Scheme}} : \overbrace{\texttt{example}}^{\texttt{DID Method}} : \underbrace{\texttt{BzCbsNYhMrjHiqZDTUASHg}}_{\texttt{Method Specific Identifier}}$$

See also:

Find out more about some of the most commonly used DID methods:

- DID:INDY
- DID:UPORT
- DID:SOV

While centralised identities and federated identities offer convenience, control remains with the identity provider [LB15]. User-centric identities such as OpenID [RR06] and OAuth [FKustersS16] improve portability but do not give complete control to the users. SSI is designed to give users full control over their digital identities, and involves guiding principles around security, controllability, and portability. In addition to providing total control, Bernabe et al. [BCHR+19] presented a classification of techniques for maintaining privacy in SSI, which included Secure Multiparty Computation and Zero-Knowledge Proofs, among others.

The three main parties involved in SSI systems are the issuer, holder and verifier, as shown in [Fig. 2.1]. The issuer issues a cryptographically signed credential to the holder, and the verifier is the entity that confirms the credential's authenticity using a decentralised data registry such as Blockchain. Holders store their credentials in secure digital wallets and can share them with other parties as needed. The holder can also create a presentation request and share it with the verifier.

SSI

Self-Sovereign Identity (SSI) is a decentralised digital identity management system which leverages blockchain technology as a data registry, allowing individuals to create, control, and share their identities securely.

Verifiable Credential

A verifiable credential is a digital artefact that provides tamper-evident, cryptographically verifiable proof of an individual's personal information or attributes.

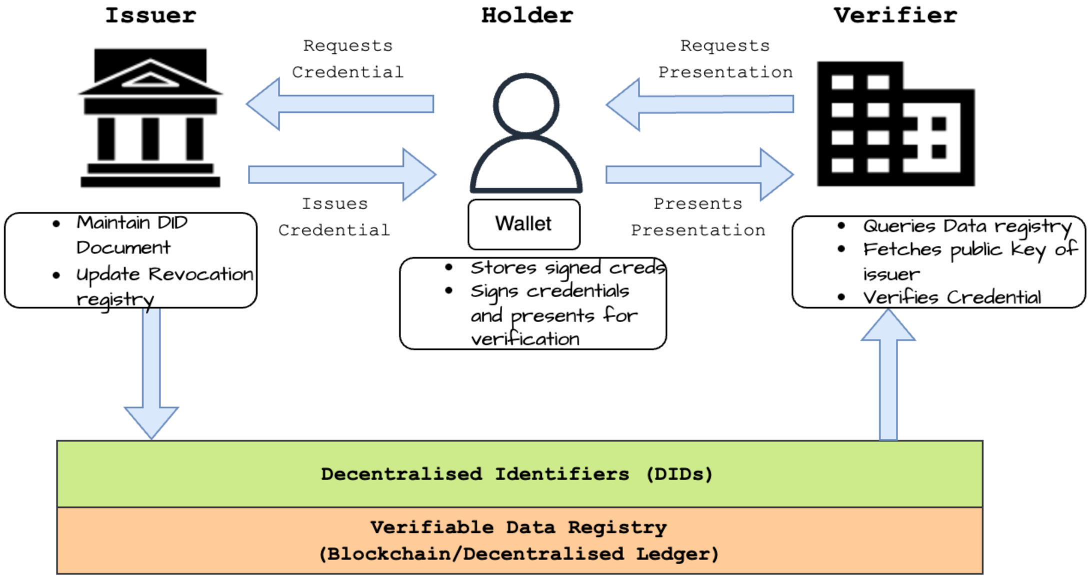
Issuer
Holder
Verifier
Requests Credential
Issues Credential
Requests Presentation
Presents Presentation
Wallet
• Maintain DID Document
• Update Revocation registry
• Stores signed creds
• Signs credentials and presents for verification
• Queries Data registry
• Fetches public key of issuer
• Verifies Credential
Decentralised Identifiers (DIDs)
Verifiable Data Registry (Blockchain/Decentralised Ledger)

Fig. 2.1: SSI entities and their relations

Click here to see how a verifiable credential actually looks like

This is a credential issued using the javascript library didkit-wasm

```
{
      "@context":[
         "https://www.w3.org/2018/credentials/v1",
         {
            "alias":"https://schema.org/name",
            "logo":"https://schema.org/logo",
            "website":"https://schema.org/url",
            "description":"https://schema.org/description",
            "BasicProfile":"https://tzprofiles.com/BasicProfile"
         }
      ],
      "id":"urn:uuid:7041d211-72c9-49fe-b6d1-d8b6b94abfe3",
      "type":[
         "VerifiableCredential",
         "BasicProfile"
      ],
      "credentialSubject":{
         "id":"did:pkh:tz:tz1N699qJqMVbMDan2r6R3QYFw42J5ydReh6",
         "alias":"TU Munich",
         "website":"Germany",
         "description":"My name",
         "logo":"Helene-Mayer-Ring 7B"
      },
      "issuer":"did:pkh:tz:tz1QRuc9BkvsBfeSGr6kJ5GCzBsrDjMedvA7",
      "issuanceDate":"2023-01-13T12:24:52.630Z",
      "proof":{
         "@context":{
            "TezosMethod2021":"https://w3id.org/security#TezosMethod2021",
            "TezosSignature2021":{
               "@context":{
                  "@protected":true,
                  "@version":1.1,
                  "challenge":"https://w3id.org/security#challenge",
                  "created":{
                     "@id":"http://purl.org/dc/terms/created",
                     "@type":"http://www.w3.org/2001/XMLSchema#dateTime"
                  },
                  "domain":"https://w3id.org/security#domain",
                  "expires":{
                     "@id":"https://w3id.org/security#expiration",
                     "@type":"http://www.w3.org/2001/XMLSchema#dateTime"
                  },
                  "id":"@id",
                  "nonce":"https://w3id.org/security#nonce",
                  "proofPurpose":{
                     "@context":{
                        "@protected":true,
                        "@version":1.1,
                        "assertionMethod":{
                           "@container":"@set",
                           "@id":"https://w3id.org/security#assertionMethod",
                           "@type":"@id"
                        },
```

(continues on next page)

(continued from previous page)

```
                       "authentication":{
                          "@container":"@set",
                          "@id":"https://w3id.org/security#authenticationMethod",
                          "@type":"@id"
                       },
                       "id":"@id",
                       "type":"@type"
                    },
                    "@id":"https://w3id.org/security#proofPurpose",
                    "@type":"@vocab"
                 },
                 "proofValue":"https://w3id.org/security#proofValue",
                 "publicKeyJwk":{
                    "@id":"https://w3id.org/security#publicKeyJwk",
                    "@type":"@json"
                 },
                 "type":"@type",
                 "verificationMethod":{
                    "@id":"https://w3id.org/security#verificationMethod",
                    "@type":"@id"
                 }
              },
              "@id":"https://w3id.org/security#TezosSignature2021"
           }
        },
        "type":"TezosSignature2021",
        "proofPurpose":"assertionMethod",
        "proofValue":
↪"edsigtaEZjPNqyWT6ZfZDTPUds7vK9RrUSFbJEpy67mAfPFYviUiWrpvhvPx2xZXRDVsPoJ3UMWjC8x1oJgY6ZziWufc87kam
↪",
        "verificationMethod":"did:pkh:tz:tz1QRuc9BkvsBfeSGr6kJ5GCzBsrDjMedvA7
↪#TezosMethod2021",
        "created":"2023-01-13T12:24:52.638Z",
        "publicKeyJwk":{
           "alg":"EdBlake2b",
           "crv":"Ed25519",
           "kty":"OKP",
           "x":"WlWqCerXoqMAMKfDWD0m2cIpvysFFqiU7L8L_I7zbfI"
        }
     }
  }
```

Nitty Gritties of SSI

- SSI solutions are designed to be blockchain-agnostic and adhere to W3C's specifications.
- The identity wallets (e.g., uPort, Trinsic, Connect.Me) are different from the digital wallets (e.g., Coinbase, Ledger, Trezor) that store cryptocurrencies in the sense that they store and manage DIDs and VCs instead of cryptocurrencies.
- To protect privacy, SSI solutions (e.g. - Hyperledger Indy and Aries) are increasingly using Zero-Knowledge Proofs (ZKPs) to prove the authenticity of credentials without revealing the actual data.
- To facilitate secure communication between different SSI components (issuer-holder-verifier), DIDComm and CHAPI protocols have been developed and heavily used.

2.2 Applications for SSI

Recent studies have demonstrated the feasibility of using zero-knowledge proofs to disclose information selectively, such as proof of vaccination status, without revealing users' identities. These studies have employed interoperable open-source tools to implement these systems globally at a minimal cost. Schlatt et al. [SSFU22] illustrates how a customer can leverage a Zero-knowledge Proof concept called 'blinded link secret' to disclose information selectively. Similarly, Barros et al. [dVBSFCustodio22] implemented a prototype of an application for presenting proof of vaccination without revealing users' identities. Furthermore, it uses interoperable open-source tools across countries to implement this system globally at a minimal cost for each country's government. The NHS Digital Staff Passport solution [LC22] employs the Sovrin Network as a public key infrastructure (PKI) to manage verifiable credentials for staff onboarding. Hospitals register on the network and use their private keys to sign credentials, while staff members utilise Evernym's Connect.Me SSI digital wallet app to store and share credentials.

Shuaib et al. [SHU+22] suggest that a blockchain-based land registry system can be combined with a self-sovereign identity (SSI) solution to provide a secure and efficient identity management system for landowners. Three existing SSI solutions: Everest, Evernym, and uPort [Ame22], were evaluated based on SSI principles [All16] to determine their compliance and effectiveness in addressing identity problems in land registry systems. The Everest platform was found to be the most compliant with the SSI principles, whereas Evernym and uPort had some limitations in terms of interoperability and user control.

Estonia is one of the few countries in the world that have managed to make e-voting a reality [SS22]. Sertkaya et al. [SRR22] proposed an EIV-AC scheme that integrates the Estonian Internet voting (EIV) scheme with anonymous credentials (AC) based on self-sovereign identity (SSI). The use of SSI-based anonymous credentials enables voters to prove their eligibility to vote without revealing their identity. The zero-knowledge proof of knowledge is used to prove that the voter has the right to vote without revealing any additional information. The EIV-AC scheme enhances the security and privacy of the EIV scheme, making it more compliant with privacy-enhancing and data minimisation regulations.

2.3 Can SSI work without Blockchain?

Blockchain is one of many options when implementing the Self-sovereign Identity system. Alternatives like IPFS, Public-key cryptography and even traditional Certificate Authorities can be used to implement SSI. However, the main advantage of using Blockchain is that it provides a decentralised and immutable ledger that can be used to store and verify credentials.

2.4 Conclusion

Self-sovereign identity can potentially revolutionise various industries, including healthcare, voting systems and many more. However, as research and development in SSI progress, it will be crucial to address interoperability, scalability, and usability challenges to realise SSI's potential in a global context fully.

CHAPTER

THREE

MOBILE THEFT PREVENTION USING BLOCKCHAIN

Key Insights

- Mobile theft is a major concern for smartphone users worldwide, with an estimated 70 million smartphones lost each year.
- Blockchain technology has the potential to provide a secure and decentralized solution to prevent mobile theft.
- The proposed model of using blockchain for mobile theft prevention offers several potential advantages over existing methods, including decentralized and tamper-proof tracking, automation of process, cross-border usage, and cost reduction.
- The smart contract enables the registration of new mobile devices and maps them to their respective phone numbers. It provides a secure and tamper-proof solution for tracking the status of mobile devices on the blockchain.
- The implementation of blockchain-based mobile theft prevention solutions provides an added layer of security that can greatly benefit mobile phone users, manufacturers, and society at large.

3.1 Introduction

Mobile theft is a major concern for smartphone users worldwide. With the increasing reliance on mobile devices for personal and professional use, the theft or loss of a smartphone can result in a significant loss of data and privacy. Studies indicate that a staggering number of smartphones, estimated at 70 million, are lost each year, with a meager 7% recovered [Hom16]. Further, company-issued smartphones are not immune to these occurrences, as research has shown that 4.3% of them are lost or stolen annually. Workplace and conference environments are the leading hotspots for smartphone theft, with 52% and 24% of devices stolen, respectively. Moreover, these numbers appear to be increasing, with recent studies indicating a rise of 39.2% between 2019 and 2021 [Hen22]. Given these alarming statistics, there is a growing need for effective mobile theft prevention measures. Blockchain technology has the potential to provide a secure and decentralized solution to prevent mobile theft. By leveraging the immutable and distributed nature of blockchain, it is possible to create a tamper-proof system that can prevent unauthorized access to mobile devices. In this article, we will explore the potential of blockchain technology for mobile theft prevention, its advantages and limitations, and the future prospects of this emerging field.

The proposed technology of using blockchain for mobile theft prevention is still in the development stage and has not yet been widely adopted on a national or international level. However, there are several companies and organizations that are exploring the use of blockchain for mobile security and anti-theft solutions. Internationally, companies such as Samsung and Huawei are researching the use of blockchain for mobile security, with Samsung filing several patents for blockchain-based mobile security solutions [For22, Hua18].

There is currently no known widespread adoption of blockchain for mobile theft prevention. However, the governments all over the world has been exploring the use of blockchain for various applications, including supply chain management and digital identity. This indicates that there is an interest in the technology and a potential for the proposed model to be adopted globally.

3.2 Rationale Behind Mobile Theft Prevention using Blockchain

Mobile theft has become a growing concern for individuals and organizations around the world. In addition to the financial loss associated with the theft, there is also a significant risk of personal data being compromised. The use of blockchain technology for mobile theft prevention offers a secure and efficient solution for preventing mobile theft [Gob18]. This technology can help individuals and organizations protect their mobile devices and personal information by providing a decentralized and tamper-proof way to track and block stolen mobile devices. By using private blockchains, the proposed model can be implemented in a way that ensures security and privacy, while also reducing the risk of fraud or malicious activity.

- **Decentralized and tamper-proof:** Blockchain technology enables a decentralized and tamper-proof system for tracking and disabling stolen mobile devices. This ensures that the information stored on the blockchain is accurate and cannot be tampered with, making it a reliable source for tracking stolen devices [Chi23].
- **Secure and private:** The proposed model uses a private blockchain network that connects the mobile manufacturing companies and their nodes [Ire21]. This helps to ensure the security of the network and the data stored in it, and also helps to maintain the privacy of the users.
- **Automation of process:** Smart contracts can be programmed to automatically disable the device once the signal is sent, reducing human error and increasing the efficiency [DD21].
- **Cross-border usage:** The proposed model can be used in cross-border cases, making it more efficient and effective than existing methods [Ram21].
- **Cost reduction:** By reducing the number of mobile thefts, the proposed model can also have a positive economic impact. This can include reducing the costs associated with mobile theft for consumers, mobile carriers, and insurance companies [Ali20].

3.3 Alternative Technologies Available under Development

- **IMEI blocking:** One of the most common methods for preventing mobile theft is to block the IMEI (International Mobile Equipment Identity) number of a stolen device. This can be done by reporting the theft to the mobile carrier, who will then blacklist the IMEI number and prevent the device from connecting to the network [Hic22].
- **SIM card blocking:** Similar to IMEI blocking, SIM card blocking involves disabling the SIM card of a stolen device. This can be done by reporting the theft to the mobile carrier, who will then deactivate the SIM card and prevent the device from connecting to the network [Tre15].
- **Remote wipe:** Some mobile devices include a remote wipe feature, which allows the device owner to remotely delete all of the data on their device if it is lost or stolen [AIT23].
- **Mobile tracking apps:** There are a variety of mobile tracking apps available that allow device owners to track the location of their device and remotely lock or wipe it if it is lost or stolen [Mar23].

In comparison, the model of using blockchain for mobile theft prevention offers several potential advantages over these existing methods. A decentralized and tamper-proof system for tracking and disabling stolen devices, and the smart contract can be programmed to automatically disable the device once the signal is sent, reducing human error and increasing the efficiency. Additionally, the proposed model can potentially work in cross-border cases, which is not possible with IMEI and SIM card blocking, and also can be integrated with other theft prevention methods.

3.4 Methodology

The smart contract enables the registration of new mobile devices and maps them to their respective phone numbers. This allows users to update the status of their mobile devices on the blockchain, indicating whether they are lost or stolen. The smart contract also allows for changes to be made to the registered mobile devices' information, such as their International Mobile Equipment Identity (IMEI) number, and to update the corresponding phone number. In this way, the smart contract provides a secure and tamper-proof solution for tracking the status of mobile devices on the blockchain.

The mobile application is designed to constantly monitor the state of the mobile device by making API calls to the blockchain. If the blockchain indicates that the device has been reported stolen, the application takes action by disabling the device's Wi-Fi and network connections and forcing it into airplane mode. By doing so, the application prevents the thief from using any of the phone's features, rendering it useless until it can be recovered by the rightful owner.

When a mobile phone is marked as stolen on the blockchain through the smart contract and later found. The owner of the phone wishes to reactivate the phone, they can connect it to a computer via USB and use USB mode to provide data to the phone. This can allow the owner to activate the phone again by providing the data through the USB based hotspot.

The below code is a smart contract written in Solidity and JavaScript that can be deployed on a blockchain network. It is designed to prevent mobile theft by using a mapping function to keep track of mobile devices using their IMEI numbers and phone numbers.

3.4.1 Smart Contract - Solidity

```
// SPDX-License-Identifier: MIT
pragma solidity 0.8.7;

contract MobileTheftPrevention{
    mapping(bytes32=>bool) private isIMEIexist;
    mapping(bytes32=>bool) private isPhoneNumberexist;
    mapping(address=>mapping(bytes32=>bytes32)) private mapAPI;
    mapping(bytes32=>bool) private isIMEIlost;

    function hash(uint _value) private pure returns(bytes32){
        return keccak256(abi.encodePacked(_value));
    }

    function addIMEI(uint _IMEI, uint _phoneNumber) public{
        require(isIMEIexist[hash(_IMEI)] == false);
        require(isPhoneNumberexist[hash(_phoneNumber)] == false);
        isIMEIexist[hash(_IMEI)] = true;
        isPhoneNumberexist[hash(_phoneNumber)] = true;
        mapAPI[msg.sender][hash(_phoneNumber)] = hash(_IMEI);
    }

    function activateLost(uint _phoneNumber) public{
        require(isIMEIexist[mapAPI[msg.sender][hash(_phoneNumber)]] == true);
        isIMEIlost[mapAPI[msg.sender][hash(_phoneNumber)]] = true;
    }

    function deactivateLost(uint _phoneNumber) public{
        require(isIMEIexist[mapAPI[msg.sender][hash(_phoneNumber)]] == true);
        isIMEIlost[mapAPI[msg.sender][hash(_phoneNumber)]] = false;
    }

    function changeIMEI(uint _IMEI, uint _phoneNumber, uint _newIMEI) public{
```

(continues on next page)

(continued from previous page)

```
        require(isIMEIexist[hash(_IMEI)] == true);
        require(isPhoneNumberexist[hash(_phoneNumber)] == true);
        require(mapAPI[msg.sender][hash(_phoneNumber)] == hash(_IMEI));
        mapAPI[msg.sender][hash(_phoneNumber)] = hash(_newIMEI);
        isIMEIexist[hash(_IMEI)] = false;
        if(isIMEIexist[hash(_newIMEI)] == false){
            isIMEIexist[hash(_IMEI)] = true;
        }
    }

    function changePhoneNumber(uint _IMEI, uint _phoneNumber, uint _newPhoneNumber)␣
↪public{
        require(isIMEIexist[hash(_IMEI)] == true);
        require(isPhoneNumberexist[hash(_phoneNumber)] == true);
        require(mapAPI[msg.sender][hash(_phoneNumber)] == hash(_IMEI));
        mapAPI[msg.sender][hash(_phoneNumber)] = hash(uint(0));
        mapAPI[msg.sender][hash(_newPhoneNumber)] = hash(_IMEI);
        isPhoneNumberexist[hash(_phoneNumber)] = false;
    }

    function checkIMEI(uint _IMEI) public view returns(bool){
        return isIMEIlost[hash(_IMEI)];
    }

}
```

3.4.2 Smart Contract - JavaScript

```
const Web3 = require('web3');
const web3 = new Web3('http://localhost:8545'); // your Blockchain client endpoint

const contractAddress = '0x123456789...'; // your contract address
const abi = [/* Smart Contract ABI */]; // your contract ABI

const contract = new web3.eth.Contract(abi, contractAddress);

const isIMEIexist = {};
const isPhoneNumberexist = {};
const mapAPI = {};
const isIMEIlost = {};

function hash(value) {
  return web3.utils.keccak256(web3.eth.abi.encodeParameter('uint256', value));
}

async function addIMEI(IMEI, phoneNumber) {
  if (!isIMEIexist[hash(IMEI)] && !isPhoneNumberexist[hash(phoneNumber)]) {
    isIMEIexist[hash(IMEI)] = true;
    isPhoneNumberexist[hash(phoneNumber)] = true;
    mapAPI[web3.eth.defaultAccount][hash(phoneNumber)] = hash(IMEI);
    await contract.methods.addIMEI(IMEI, phoneNumber).send({ from: web3.eth.
↪defaultAccount });
  }
}
```

(continues on next page)

(continued from previous page)

```
async function activateLost(phoneNumber) {
  const IMEI = mapAPI[web3.eth.defaultAccount][hash(phoneNumber)];
  if (isIMEIexist[IMEI]) {
    isIMEIlost[IMEI] = true;
    await contract.methods.activateLost(phoneNumber).send({ from: web3.eth.defaultAccount });
  }
}

async function deactivateLost(phoneNumber) {
  const IMEI = mapAPI[web3.eth.defaultAccount][hash(phoneNumber)];
  if (isIMEIexist[IMEI]) {
    isIMEIlost[IMEI] = false;
    await contract.methods.deactivateLost(phoneNumber).send({ from: web3.eth.defaultAccount });
  }
}

async function changeIMEI(IMEI, phoneNumber, newIMEI) {
  if (isIMEIexist[hash(IMEI)] && isPhoneNumberexist[hash(phoneNumber)] && mapAPI[web3.eth.defaultAccount][hash(phoneNumber)] === hash(IMEI)) {
    mapAPI[web3.eth.defaultAccount][hash(phoneNumber)] = hash(newIMEI);
    isIMEIexist[hash(IMEI)] = false;
    if (!isIMEIexist[hash(newIMEI)]) {
      isIMEIexist[hash(newIMEI)] = true;
    }
    await contract.methods.changeIMEI(IMEI, phoneNumber, newIMEI).send({ from: web3.eth.defaultAccount });
  }
}

async function changePhoneNumber(IMEI, phoneNumber, newPhoneNumber) {
  if (isIMEIexist[hash(IMEI)] && isPhoneNumberexist[hash(phoneNumber)] && mapAPI[web3.eth.defaultAccount][hash(phoneNumber)] === hash(IMEI)) {
    mapAPI[web3.eth.defaultAccount][hash(phoneNumber)] = hash(0);
    mapAPI[web3.eth.defaultAccount][hash(newPhoneNumber)] = hash(IMEI);
    isPhoneNumberexist[hash(phoneNumber)] = false;
    await contract.methods.changePhoneNumber(IMEI, phoneNumber, newPhoneNumber).send({ from: web3.eth.defaultAccount });
  }
}

async function checkIMEI(IMEI) {
  return isIMEIlost[hash(IMEI)];
}

module.exports = {
  addIMEI,
  activateLost,
  deactivateLost,
  changeIMEI,
  changePhoneNumber,
  checkIMEI
};
```

The smart contract consists of six functions that can be called by authorized users.

- `addIMEI()` allows users to add their mobile devices to the blockchain by passing in their IMEI and phone numbers. The function first checks if the IMEI and phone numbers already exist on the blockchain, and if not, it adds the device to the mapping function.
- `activateLost()` is used to activate the lost mode of a mobile device. The function checks if the IMEI number of the device exists on the blockchain and if it does, it sets the value of `isIMEIlost` to true, indicating that the device is lost.
- `deactivateLost()` is used to deactivate the lost mode of a mobile device. The function checks if the IMEI number of the device exists on the blockchain and if it does, it sets the value of `isIMEIlost` to false, indicating that the device is no longer lost.
- `changeIMEI()` allows users to change the IMEI number of their device. The function checks if the old IMEI and phone number exists on the blockchain and if it does, it replaces the old IMEI with the new one.
- `changePhoneNumber()` allows users to change the phone number associated with their device. The function checks if the old IMEI and phone number exists on the blockchain and if it does, it replaces the old phone number with the new one.
- `checkIMEI()` is a view function that allows anyone to check if a particular device is lost by passing in the IMEI number of the device. The function returns true if the device is lost, and false if it is not.

3.5 Potential Impact

As the world continues to advance technologically, mobile phone theft has become a common issue that affects many people. However, with the implementation of a blockchain-based mobile theft prevention solution, it is possible to mitigate this problem.

3.6 Potential Impact on Users and Mobile Manufacturers

For users, this solution provides an added layer of security, ensuring that their mobile devices cannot be easily used if they are lost or stolen. With the mobile application continuously reading the state of the mobile through API calls to the blockchain, it is possible to detect if the mobile is stolen, and take appropriate actions to disable the mobile network, Wi-Fi, and force activate airplane mode, preventing the thief from using any of the phone's functionalities.

For mobile manufacturers, implementing blockchain-based mobile theft prevention solution will increase customer satisfaction and retention as users are likely to be attracted to the added security feature. This, in turn, will lead to an increase in sales and profits.

3.7 Potential Economic and Social Benefits

The implementation of blockchain-based mobile theft prevention solutions will lead to a reduction in mobile phone theft and related crimes. This will result in a decrease in the costs of replacing stolen or lost mobile phones, and a corresponding increase in the amount of money available for investment in other areas of the economy. Additionally, it can also help to reduce insurance premiums for mobile phone owners, leading to savings for consumers.

On a social level, it can help to reduce the fear of being robbed or mugged and reduce the potential for violent confrontations between victims and thieves. This can lead to an overall improvement in public safety and security.

3.8 Future Possibilities and Extensions

The implementation of this blockchain-based mobile theft prevention solution has future possibilities and extensions. It can be extended to other mobile devices like laptops, tablets, and smartwatches, further increasing the level of security for users. Additionally, it can be integrated with existing law enforcement agencies to enhance the tracking of lost or stolen mobile devices. This will make it easier for law enforcement to recover stolen mobile devices and increase the likelihood of criminals being brought to justice.

In conclusion, the implementation of blockchain-based mobile theft prevention solutions provides an added layer of security that can greatly benefit mobile phone users, manufacturers, and society at large. The potential for future extensions and possibilities only adds to its value, making it an ideal solution for improving the safety and security of mobile devices.

CHAPTER

FOUR

REFERENCES

BIBLIOGRAPHY

[Ali20] **missing journal in Ali2020costreduction**

[All16] Christopher Allen. The path to self-sovereign identity. *Life With Alacrity*, 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[Ame22] New America. Three self-sovereign identity platforms to watch. *New America*, 2022. URL: https://www.newamerica.org/future-land-housing/reports/nail-finds-hammer/three-self-sovereign-identity-platforms-to-watch/.

[AIT23] Asha Iyengar, Jeff Borsecnik and Team. Perform a remote wipe on a mobile phone. *Microsoft*, 2023. URL: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-2019.

[BSP+22a] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Alexander Rieger, and Gilbert Fridgen. Defi, not so decentralized: the measured distribution of voting rights. *Hawaii International Conference on System Sciences (HICSS)*, 2022.

[BSP+22b] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Johannes Sedlmeir, and Gilbert Fridgen. Decentralised finance's unregulated governance: minority rule in the digital wild west. *Available at SSRN*, 2022.

[BCHR+19] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-preserving solutions for blockchain: review and challenges. *IEEE Access*, 7:164908–164940, 2019.

[Chi23] Chirag. Blockchain: the technology revolutionizing mobile app security. *Appinventive*, 2023. URL: https://appinventiv.com/blog/blockchain-technology-revolutionizing-mobile-app-security/.

[dVBSFCustodio22] Mauricio de Vasconcelos Barros, Frederico Schardong, and Ricardo Felipe Custódio. Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass. *Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass*, 2022.

[DD21] Utpal Biswas Debashis Das, Sourav Banerjee. A secure vehicle theft detection framework using blockchain and smart contract. *Springer*, 2021. URL: https://doi.org/10.1007/s12083-020-01022-0.

[EAw22] Hassan Hamid Ekal and Shams N Abdul-wahab. Defi governance and decision-making on blockchain. *Mesopotamian Journal of Computer Science*, 2022:9–16, 2022.

[FKustersS16] Daniel Fett, Ralf Küsters, and Guido Schmitz. A comprehensive formal security analysis of oauth 2.0. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1204–1215. 2016.

[For22] Savannah Fortis. Samsung uses blockchain-based security for devices in its network. *Cointelegraph*, 2022. URL: https://cointelegraph.com/news/web3-protection-platform-introduces-improved-detection-mechanics-in-latest-update.

[Gob18] Andreas Göbel. Using blockchain to prevent mobile phone theft. *Camelot*, 2018. URL: https://blog.camelot-group.com/2018/12/using-blockchain-to-prevent-mobile-phone-theft/.

[Hen22] Beatriz Henriquez. Mobile theft and loss report - 2020/2021 edition. *PREY Project*, 2022. URL: https://preyproject.com/blog/mobile-theft-and-loss-report-2020-2021-edition.

[Hic22] Jacob Hicks. How to block a stolen iphone with an imei number. *DeviceTests*, 2022. URL: https://devicetests.com/how-to-block-a-stolen-iphone-with-an-imei-number.

[Hom16] Elaine J. Hom. Mobile device security: startling statistics on data loss and data breaches. *ChannelProNetwork*, 2016. URL: https://www.channelpronetwork.com/article/mobile-device-security-startling-statistics-data-loss-and-data-breaches.

[Hua18] Huawei. Huawei blockchain whitepaper. *Huawei*, 2018. URL: https://www.huaweicloud.com/content/dam/cloudbu-site/archive/hk/en-us/about/analyst-reports/images/4-201804-Huawei%20Blockchain%20Whitepaper-en.pdf.

[Ire21] Gwyneth Iredale. The rise of private blockchain technologies. *101 Blockchains*, 2021. URL: https://101blockchains.com/private-blockchain/.

[JvWR21] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. How decentralized is the governance of blockchain-based finance: empirical evidence from four governance token distributions. *arXiv preprint arXiv:2102.10096*, 2021.

[JC23] CLAIRE CASHER JULIA CLARK, ANNA DIOFASI. 850 million people globally don't have id—why this matters and what we can do about it. *World Bank*, 2023. URL: https://blogs.worldbank.org/digital-development/850-million-people-globally-dont-have-id-why-matters-and-what-we-can-do-about.

[LC22] Mary Lacity and Erran Carmel. Implementing self-sovereign identity (ssi) for a digital staff passport at uk nhs. *University of Arkansas*, 2022.

[LB15] Maryline Laurent and Samia Bouzefrane. *Digital identity management*. Elsevier, 2015.

[Mar23] Karen Marcus. The 8 best phone tracker apps of 2023. *Lifewire*, 2023. URL: https://learn.microsoft.com/en-us/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-2019.

[MKB22] Vijay Mohan, Peyman Khezr, and Chris Berg. Voting with time commitment for decentralized governance: bond voting as a sybil-resistant mechanism. *Available at SSRN*, 2022.

[Nab23] Kelsie Nabben. Governance by algorithms, governance of algorithms: human-machine politics in decentralised autonomous organisations (daos). *puntOorg International Journal*, 8(1):36–54, 2023.

[Ram21] Murali Ramakrishnan. How blockchain works in cross-border payments. *Springer*, 2021. URL: https://blogs.oracle.com/financialservices/post/how-blockchain-works-in-cross-border-payments-.

[RR06] David Recordon and Drummond Reed. Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, 11–16. 2006.

[SSFU22] Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, and Nils Urbach. Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity. *Information & Management*, 59(7):103553, 2022.

[SS22] Cyber Security and Society. Estonia leads world in making digital voting a reality. *Cyber Security and Society*, 2022. URL: https://www.ft.com/content/b4425338-6207-49a0-bbfb-6ae5460fc1c1.

[SRR22] Isa Sertkaya, Peter Roenne, and Peter YA Ryan. Estonian internet voting with anonymous credentials. *Turkish Journal of Electrical Engineering and Computer Sciences*, 30(2):420–435, 2022.

[SHU+22] Mohammed Shuaib, Noor Hafizah Hassan, Sahnius Usman, Shadab Alam, Surbhi Bhatia, Arwa Mashat, Adarsh Kumar, and Manoj Kumar. Self-sovereign identity solution for blockchain-based land registry system: a comparison. *Mobile Information Systems*, 2022:1–17, 2022.

[S+] K Stroponiati and others. Decentralized governance in defi: examples and pitfalls. squarespace. retrieved december 30, 2022.

[Tre15] Mobile ICT Trends. Erasing your device, blocking your sim card: how to be prepared when your phone gets stolen. *econocom*, 2015. URL: https://blog.econocom.com/en/blog/what-to-do-if-your-mobile-device-gets-stolen-how-do-you-block-your-sim-card-heres-how-to-be-prepared-for-the-loss-

[XPFL23] Jiahua Xu, Daniel Perez, Yebo Feng, and Benjamin Livshits. Auto. gov: learning-based on-chain governance for decentralized finance (defi). *arXiv preprint arXiv:2302.09551*, 2023.