A Blockchain Based Self-Sovereign Identity Verification System

Ronnie Mulandi 138617 CNS

Supervisor Name

Dr. Vitalis Ozianyi

Submitted in Partial Fulfillment of the Requirements of the Bachelor of Science in Computer

Networks and Cybersecurity at the Strathmore University School of Computing and Engineering

Science Strathmore University Nairobi,

Kenya

May 2023

Declaration

I would like to declare that this research project is my original work and has not been presented for award of a degree or for any similar purpose in any other institution

Student Name: Ronnie Mulandi Mutisya

Admission Number: 138617

Signature: ____________________ Date: ___________________

This research project has been submitted with my approval as University supervisor

Dr. Vitalis Ozianyi

Supervisor Signature: ____________________ Date: _________________________

Strathmore University

Acknowledgement

I am highly indebted to Strathmore University for its guidance and constant supervision as well as for providing necessary information regarding the project & also for the support in completing the project.

I would like to express my sincere gratitude to my supervisors Dr. Vitalis Ozianyi for providing their invaluable guidance, comments and suggestions throughout the course of the project.

Abstract

In today's digital age, the management of personal identity and data has become a significant challenge. Traditional identity verification methods often involve large corporations that store and control personal data. These companies often collect and monetize user data through targeted advertising, data analytics, or other means which can lead to privacy and security concerns if these centralized databases are compromised. To address this challenge, this project proposes the development of a blockchain-based self-sovereign identity verification system that enables individuals to maintain control over their personal data and privacy.

The system will leverage blockchain technology, smart contracts, data encryption, and privacy-enhancing technologies to create a tamper-proof and immutable record of a user's digital identity and personal data. Adopting industry standards and interoperability protocols to ensure compatibility with other identity verification systems and services. A User-centered design approach will be used to ensure that the system is easy to use and meets the needs and preferences of users. To make sure the system is reliable, secure, and effective, extensive testing will be done throughout all stages of development.

This project will contribute to the development of a more secure and user-centric approach to identity management and verification, utilizing the latest technologies to address the challenges of privacy, efficiency, security, and user control improving the overall user experience and enhancing trust and security in digital transactions.

Table of Contents

Contents

Table of Figures

List of Abbreviations

SSI – Self Sovereign Identity

DLT – Distributed Ledger Technology

IdM – Identity Management

IAM – Identity Access Management

ZKP - Zero-Knowledge Proof protocols

DID – Digital Identifier

OOAD - Object-Oriented Analysis and Design

CHAPTER 1: INTRODUCTION

1.1 Background information

"*Who or what someone or something is*" is the definition of *identity* by the Oxford dictionary (*Oxford English Dictionary (Online)*, n.d.). Digital identities are the digital counterpart of our identity and a crucial part of our daily digital life. Every individual that uses online services owns several of those digital representations of themselves. Besides for online services, digital identities are also used as the digital counterpart of physical identity cards. These types of digital identities can be used not only to identify a user to an online service, but also to real persons for various services. This information is held by various organizations, including social media platforms, e-commerce sites, financial institutions, and government agencies. While these organizations are responsible for protecting individuals' data, the reality is that personal data is vulnerable to security breaches, hacking, and misuse.

In some perfect world individuals would have complete control over their personal data and could easily and securely prove their identity in any context without the need for a centralized verification system. Additionally, all organizations and service providers would prioritize user privacy and security, ensuring that personal data is protected at all times and only used for legitimate purposes.

In 2008, a researcher or group of researchers under Nakamoto Satoshi published the well-known paper "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto, 2009), which introduced the idea of Blockchain technology. This new technology provided huge potential in various fields allowing a new identity model to evolve, the so-called Self-Sovereign Identity (SSI).

The concept of self-sovereign identity (SSI) describes an identity management system created to operate independently of third-party public or private actors, based on decentralized technological architectures, and designed to prioritize user security, privacy, individual autonomy and self-empowerment. (Giannopoulou & Wang, 2021). SSI allows individuals to create a digital identity on the blockchain that is linked to their real-world identity. This digital identity can then be used to prove their identity in various contexts, such as accessing online services, signing contracts, and voting. The user has complete control over their personal information and can choose which pieces of data to share and with whom. This approach not only enhances user privacy and security but also reduces the reliance on centralized identity providers.

This project will involve thorough research into the concepts of self-sovereign identity and blockchain technology allowing understanding the theoretical foundations and existing implementation of SSI systems. Designing a system that combines the decentralized nature of blockchain technology with the principles of SSI to empower individuals with control over their personal identity information, ensuring privacy, security, and user autonomy. Smart contracts will be used to automate the verification process by setting up a set of rules or conditions that must be met before a transaction can be executed, facilitating trustless transactions in the blockchain and eliminating the need for intermediaries and reducing the risk of fraud. Data encryption to safeguard sensitive user information and privacy-enhancing technologies such as zero knowledge proof will allow for the verification of information without revealing the underlying data, enhancing privacy and confidentiality.

The combination of these technologies in the project aims to provide a secure and user-centric identity verification system that is resistant to tampering, fraud, and identity theft. While providing individuals with greater control over their personal identity information.

1.2 Problem Statement

The current centralized approach to identity management and verification is plagued with numerous problems, including lack of user control over personal data, susceptibility to data breaches and identity theft. Time-consuming and repetitive verification processes have become the new normal. In these systems, individuals are required to undergo redundant identity verification procedures when interacting with different service providers or platforms. This redundancy not only wastes time and resources but also increases the potential for errors and delays in accessing services or conducting transactions.

This repetition of identity verification not only burdens individuals with the need to repeatedly provide sensitive personal data raising concerns about privacy and data security but also from the perspective of organizations and service providers, the reliance on repetitive identity verification leads to administrative overhead, increased costs, and slower customer onboarding or service delivery, hampering the efficiency of operations and creating friction in user experiences.

The problem lies in the lack of a unified and interoperable identity verification framework, where verified identities can be easily and securely shared across multiple entities. Therefore, there is a pressing need for a decentralized and interoperable identity verification system that eliminates the redundancy of verification processes. Such a system would allow individuals to establish and maintain a verified identity once, which can be securely shared across multiple entities, streamlining processes, enhancing efficiency, and safeguarding privacy. The Self Sovereign Identity Verification System project seeks to address this problem of repetitive verification in traditional centralized identification verification systems by developing a decentralized and interoperable framework for identity verification will providing user control over their personal data and privacy.

1.3 Objectives

1.3.1 General Objective

The general objective of this project is to develop a Self-Sovereign Identity Verification System using blockchain technology and other privacy-enhancing technologies.

1.3.2 Specific Objectives

i. To review literature on blockchain technology and its relation to existing identity management and verification systems.
ii. To evaluate various Self Sovereign Identity (SSI) frameworks and protocols for suitability and effectiveness in the Self-Sovereign Identity verification system
iii. To design and develop a prototype of the self-sovereign identity verification system.
iv. To conduct thorough testing and evaluation of the Self-Sovereign Identity Verification System.

1.4 Research Questions

i. How does blockchain technology ensure data privacy, security, and immutability in identity management systems?

ii. What are the different SSI frameworks and protocols available for implementing Self Sovereign Identity solutions?

iii. What are the technical requirements and architecture needed to support the secure storage, management, and verification of identity credentials within the system?

iv. How does the system compare to traditional centralized identity verification systems in terms of efficiency, privacy protection, and user control?

1.5 Justification

Traditional centralized identification systems suffer from repetitive verification processes which pose significant challenges leading to wasted time, redundant data collection, and privacy concerns. By leveraging blockchain technology and self-sovereign identity (SSI) frameworks, this project aims to revolutionize the way identities are managed and verified. The proposed system will empower individuals with ownership and control over their identity information, streamline verification processes, enhance data privacy and security, and establish a decentralized and interoperable framework. By eliminating redundant verifications, the project will improve efficiency, reduce costs, and provide individuals with greater autonomy and trust in the management of their identities.

1.6 Scope and Delimitations

The scope of this project includes the design, development, and evaluation of a prototype Self-Sovereign Identity Verification System using blockchain technology and other privacy-enhancing technologies. The project will focus on the technical aspects of the Self-Sovereign Identity Verification System, including the design and implementation of the blockchain infrastructure, smart contracts, and integration of privacy-enhancing technologies. It will also involve the development of a user interface that allows individuals to manage their digital identities and selectively share information. The use of SSI has been tied to the use of a blockchain. However, SSI is blockchain-adjacent, but not blockchain-dependent (Giannopoulou & Wang, 2021). The project explores the integration of blockchain technology as one of the possible technologies for implementing SSI overlooking other decentralized or distributed technologies that can support the principles of SSI, such as distributed ledger technology (DLT) or peer-to-peer networks. The focus will be on developing a functional prototype and conducting testing and evaluation within a controlled setting. The project aims to create a proof-of-concept implementation that demonstrates the feasibility and effectiveness of the proposed system.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Blockchains can be informally defined as distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.

The core ideas behind blockchain technology emerged in the late 1980s and early 1990s. In 1989, Leslie Lamport developed the Paxos protocol, and in 1990 submitted a paper describing a consensus model for reaching agreement on a result in a network of computers where the computers or network itself may be unreliable. In 1991, a signed chain of information was used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed. These concepts were combined and applied to electronic cash in 2008 and described in the paper, *Bitcoin: A Peer to Peer Electronic Cash System,* which was published pseudonymously by Satoshi Nakamoto, and then later in 2009 with the establishment of the Bitcoin cryptocurrency blockchain network. Nakamoto's paper contained the blueprint that most modern cryptocurrency schemes follow.

The use of a blockchain enabled Bitcoin to be implemented in a distributed fashion such that no single user controlled the electronic cash and no single point of failure existed; this promoted its use. Its primary benefit was to enable direct transactions between users without the need for a trusted third party. By using a blockchain and consensus-based maintenance, a self-policing mechanism was created that ensured that only valid transactions and blocks were added to the blockchain. The blockchain enabled users to be pseudonymous. This means that users are anonymous, but their account identifiers are not; additionally, all transactions are publicly visible.

With pseudonymity it was essential to have mechanisms to create trust in an environment where users could not be easily identified. Prior to the use of blockchain technology, this trust was typically delivered through intermediaries trusted by both parties. Without trusted intermediaries, the needed trust within a blockchain network is enabled by four key characteristics of blockchain technology, described below:

- Ledger – the technology uses an append only ledger to provide full transactional history. Unlike traditional databases, transactions and values in a blockchain are not overridden.
- Secure – blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered with, and that the data within the ledger is attestable.
- Shared – the ledger is shared amongst multiple participants. This provides transparency across the node participants in the blockchain network.
- Distributed – the blockchain can be distributed. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain is reduced.

For blockchain networks that allow anyone to anonymously create accounts and participate (called permissionless blockchain networks), these capabilities deliver a level of trust amongst parties with no prior knowledge of one another; this trust can enable individuals and organizations to transact directly, which may result in transactions being delivered faster and at lower costs. For a blockchain network that more tightly controls access (called permissioned blockchain networks), where some trust may be present among users, these capabilities help to bolster that trust.

2.2 Digital Identity using Blockchain

Blockchain technology has started with crypto currency but it has been expanded its use in cyber-physical systems, data privacy, and digital identity in this cyber world. In this digital age, the term digital identity comes to the forefront.

The process of Digital Identity involves an issuer, a verifier, a decentralized ledger and digital identity holder. Identity is any personal data, such as name or date of birth (DOB) that can be attested by a trusted authority. So, we can understand the process in a way like entities that issue credentials such as department of motor vehicles, election commissioner, hospitals, income tax department etc., are known as issuers. Owners of the credentials are known as users or holders. Any entity that the owner presents a claim to, so that the owner can establish some aspects of its identity, is a verifier. (Jena & Barik, 2023)

Digital identities require management, the so-called Identity Management (IdM), that is also known as Identity and Access Management (IAM). IdM defines the stakeholder of the identity system, the lifecycle of a digital identity, and also the access management. (Abraham, 2022) Access management the essential component in implementing a blockchain based system.

Blockchain networks can be categorized based on their permission model, which determines who can maintain them (i.e. publish blocks). If anyone can publish a new block, it is permissionless. If only particular users can publish blocks, it is permissioned. Permissioned blockchain networks are often deployed for a group of organizations and individuals, typically referred to as a consortium.

A Private Blockchain, is a permissioned blockchain. It authorizes the participates of the network and the transactions they can do. It is authorized that who can write and read data on a private blockchain. In this process, the initial step is to establish one's identity. It is the need to know who is connected to the blockchain. If the user is anonymous, defining rules for the type of data the user can commit and read from the ledger becomes complicated, if not impossible. Permissioned Blockchain advantage is that it is known who a user is, what organization they're affiliated with, and what their job is. It is presumed that they'll behave equally because if they don't, an administrator would know who's misbehaving and they'll know they'll pay the price. (Garg & Vashisht, 2021)

Some other advantages of Private blockchains are

- *Faster Transactions*

  The output is faster when the nodes are distributed locally but there are fewer nodes participating in the ledger.

- *Enterprise Permissioned*

  Blockchain resource access is controlled by the organization, making it private and/or permissioned.

- *Better Scalability*

  The ability to add resources and nodes by request can be a huge benefit.

Blockchain network users submit candidate transactions to the blockchain network via software (desktop applications, smartphone applications, digital wallets, web services, etc.). The software sends these transactions to a node or nodes within the blockchain network. The chosen nodes may be non-publishing full nodes as well as publishing nodes. The submitted transactions are then propagated to the other nodes in the network, but this by itself does not place the transaction in the blockchain. For many blockchain implementations, once a pending transaction has been distributed to nodes, it must then wait in a queue until it is added to the blockchain by a publishing node. (Yaga et al., 2018)

When a user joins a blockchain network, they agree to the initial state of the system. This is recorded in the only pre-configured block, the genesis block. Every blockchain network has a published genesis block and every block must be added to the blockchain after it, based on the agreed-upon consensus model. Consensus model is the aspect of blockchain technology determining which user publishes the next block.

The proof of authority (also referred to as proof of identity) consensus model relies on the partial trust of publishing nodes through their known link to real world identities. Publishing nodes must have their identities proven and verifiable within the blockchain network (e.g., identifying documents which have been verified and notarized and included on the blockchain). The idea is that the publishing node is staking its identity/reputation to publish new blocks. Blockchain network users directly affect a publishing node's reputation based on the publishing node's behavior. Publishing nodes can lose reputation by acting in a way that the blockchain network users disagree with, just as they can gain reputation by acting in a manner that the blockchain network users agree with. The lower the reputation, the less likelihood of being able to publish a block. Therefore, it is in the interest of a publishing node to maintain a high reputation. (Yaga et al., 2018)

With regards to identity management and verification on blockchain, the project will explore the use of Proof of Authority (PoA) consensus mechanism, digital identities, and permissioned blockchains. (Jamal et al., 2019) By utilizing PoA, the project aims to ensure faster transaction processing and improved scalability, making it suitable for applications where efficiency and trustworthiness are essential. Digital identities will play a pivotal role in the project, allowing individuals to establish and control their unique digital personas on the blockchain. These digital identities will be linked to real-world identities, enabling secure and verifiable interactions within the system. Additionally, the project will leverage permissioned blockchains, which restrict network participation to approved entities, ensuring that only trusted actors can validate transactions and maintain the integrity of the system. This approach provides an added layer of control and governance, making it suitable for use cases that require tighter access management and privacy controls.

2.3 Self-Sovereign Identity Frameworks

The concept of SSI has been elaborated as an expression of personal digital sovereignty by (Allen, n.d.). He used it to describe a principle-based framework that would create a decentralized system of user-centric, self-administered, interoperable digital identities. By thoroughly examining and comparing the various SSI frameworks. valuable insights will provide a guide in selecting the most suitable framework to achieve the project's objectives effectively.

Hyperledger Aries, a library within the broader Hyperledger project, offers a shared and reusable toolkit for creating, transmitting, and storing verifiable digital credentials. It provides an infrastructure that facilitates trusted peer-to-peer interactions based on decentralized identities and verifiable credentials. With its comprehensive protocol definition, tools, and reference implementations, Hyperledger Aries serves as a robust foundation for developing SSI systems.

uPort, developed by ConsenSys, is an open-source SSI platform built on Ethereum. It provides individuals with a mobile application and developer tools to create and manage their digital identities. Emphasizing privacy and user control, uPort enables selective disclosure of personal information and supports decentralized identity management and secure authentication.(*UPort*, n.d.)

Microsoft DID (Decentralized Identity) is a framework and set of protocols developed by Microsoft to enable the creation and management of decentralized identities. Leveraging blockchain technology, Microsoft DID offers tamper-proof and verifiable identities. It prioritizes interoperability and integration with existing identity systems, allowing users to seamlessly manage their identities across different platforms and services.(Microsoft, n.d.)

Evernym is a leading provider of SSI solutions, best known for its Sovrin Network, an open-source public utility for self-sovereign identity. Evernym's platform offers a secure and scalable infrastructure for decentralized identity management. It places a strong emphasis on privacy, user control, and interoperability, empowering individuals to securely manage and share their personal data.

Blockstack is a decentralized computing platform that incorporates self-sovereign identity principles. By leveraging blockchain technology and distributed storage, Blockstack enables users to create and manage their identities. It provides tools and protocols for secure and private identity management, facilitating user control over their data and enabling interaction with various decentralized applications.

These frameworks offer features such as Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), Zero-Knowledge Proof (ZKP) protocols, and Identity Hubs. The following table provides a comprehensive comparison of various Self-Sovereign Identity (SSI) frameworks, highlighting their key features, functionalities, and implementation considerations. This comparison aims to assist in the evaluation and selection of the most suitable SSI framework for the Self-Sovereign Identity Verification System project.

Table 1: Comparison of SSI Frameworks

Framework	**Description**	**Key Features**	**Implementation**
Sovrin	An open-source SSI framework built on a public permissioned ledger (Sovrin Network).	Decentralized identifiers (DIDs), verifiable credentials, revocation, selective disclosure, governance	Hyperledger Indy, Hyperledger Aries
UPort	A decentralized identity platform leveraging Ethereum blockchain.	DIDs, verifiable credentials, mobile wallet	Ethereum blockchain
Microsoft DID	A set of tools and libraries provided by Microsoft for building decentralized identities.	DIDs, verifiable credentials, interoperability	Azure Blockchain Service, Ethereum
Evernym	A private SSI framework offering enterprise-grade identity solutions.	DIDs, verifiable credentials, privacy-preserving	Sovrin Network, Hyperledger Indy
Blockstack	A decentralized identity protocol utilizing blockchain technology.	DIDs, verifiable credentials, data storage	Bitcoin blockchain, Gaia storage system
Jolocom	A self-sovereign identity framework using a custom-built blockchain.	DIDs, verifiable credentials, wallet	Jolocom blockchain, Ethereum

2.4 CONCEPTUAL FRAMEWORK

The conceptual framework of the Self-Sovereign Identity verification system for verifying university credentials consists of the following components:

i. Issuer: Authoritative entities such as universities or government institutions that issue verifiable credentials to individuals.

ii. Subject: The individual whose credentials are being verified. Credentials are linked to the subject’s digital identity

iii. Verifier: Entities such as employers or application offices that need to verify the authenticity of an individual's credentials.

iv. Blockchain Network: The underlying infrastructure that provides a decentralized and immutable ledger for recording transactions and credential data.

v. Smart Contracts: Programmable code deployed on the blockchain network that facilitates the execution of predefined actions based on predefined conditions and rules.

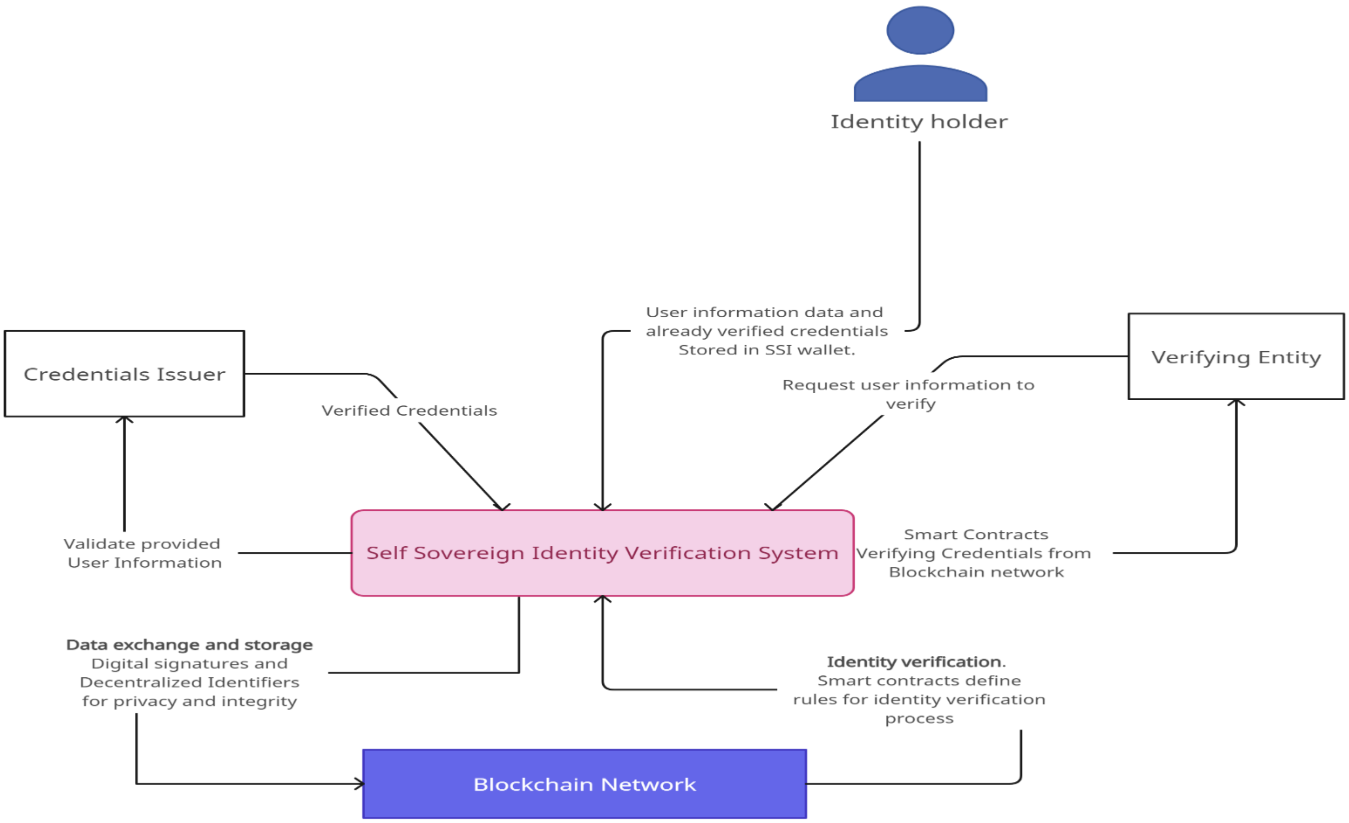
Identity holder
User information data and already verified credentials Stored in SSI wallet.
Credentials Issuer
Verified Credentials
Verifying Entity
Request user information to verify
Validate provided User Information
Self Sovereign Identity Verification System
Smart Contracts Verifying Credentials from Blockchain network
Data exchange and storage
Digital signatures and Decentralized Identifiers for privacy and integrity
Identity verification.
Smart contracts define rules for identity verification process
Blockchain Network

Figure 1: Conceptual framework

The operation of the Self-Sovereign Identity verification system involves the following steps:

i. User Registration: Individuals create a user account and a digital wallet within the system, establishing their digital identity.

ii. Credential Issuance: The credential issuer generates verifiable credentials for the individual, including details of their educational qualifications, degrees, and certifications. These credentials are digitally signed by the issuer and stored in the user's wallet.

iii. Verification Request: When the individual needs to verify their university credentials, they present the relevant credentials from their user wallet to the verifier.

iv. Verification Process: The verifier uses cryptographic techniques to verify the authenticity and integrity of the presented credentials. They perform checks on digital signatures, cross-reference the credentials with trusted sources, and validate the information against predefined rules and standards.

v. Transaction Recording: Once the verification process is successfully completed, a transaction is recorded on the blockchain network. This transaction includes the details of the verification, such as the verifier's identity, the credential subject's identity, and the verification outcome.

CHAPTER 3: METHODOLOGY

3.1 Introduction

This chapter presents the methodology adopted for the development and implementation of the Self-Sovereign Identity Verification System. The chosen methodology is Object-Oriented Analysis and Design (OOAD), which provides a structured approach to software development, focusing on capturing requirements, modeling the system, and designing robust and scalable solutions. This chapter also discusses the justification for selecting the OOAD methodology, as well as the development tools and expected deliverables for the project.

3.2 Methodology

The Object-Oriented Analysis and Design (OOAD) methodology will be employed for the development of the Self-Sovereign Identity Verification System. This methodology follows a systematic and iterative process that involves identifying the system's objects, defining their relationships, and designing their behaviors to achieve the desired functionality. The OOAD methodology comprises the following key phases:

1. Requirements Gathering: This phase involves understanding the information needed, validation processes, privacy requirements, and interoperability considerations.
2. System Analysis: Based on the gathered requirements, the system's objects, attributes, and relationships will be identified and analyzed. Use case diagrams, class diagrams, and activity diagrams will be used to model the system's structure and behavior. This phase will focus on understanding the interactions between entities such as users, educational institutions, and verifiers.
3. System Design: The system design phase will translate the analysis results into a detailed design that defines the architecture, modules, and interfaces of the Self-Sovereign Identity Verification System. Design patterns and security considerations will be incorporated to ensure the system's integrity and protection of sensitive information.
4. Implementation: The design specifications will be implemented using object-oriented programming languages and frameworks suitable for self-sovereign identity solutions. Technologies like Hyperledger Indy and Hyperledger Aries may be leveraged to build the necessary infrastructure and functionalities. The implementation phase will involve

coding the system's modules, integrating components, and conducting unit testing to ensure proper functionality.

5. Testing and Quality Assurance: Comprehensive testing strategies will be employed to verify the Self-Sovereign Identity Verification System's accuracy, reliability, and security. This will include unit testing, integration testing, system testing, and user acceptance testing. Quality assurance practices, such as code reviews and vulnerability assessments, will be followed to maintain a high level of software quality.
6. Deployment and Maintenance: The Self-Sovereign Identity Verification System will be deployed in a production environment, and ongoing maintenance and support activities will be performed to address any issues, provide updates, and incorporate user feedback.

3.3 Justification for the Methodology

The decision to employ the Object-Oriented Analysis and Design (OOAD) methodology for the development of the Self-Sovereign Identity Verification System is based on several justifications:

1. Modularity and Reusability: The OOAD methodology emphasizes modular design, allowing the system to be broken down into manageable and reusable components. This modularity promotes code reusability, reduces development time, and enhances maintainability.
2. Clear and Structured Analysis: OOAD provides a structured approach to system analysis, enabling the requirements to be captured and documented comprehensively. The use of diagrams and models, such as use case diagrams and class diagrams, helps visualize the system's structure, behavior, and interactions.
3. Object-Oriented Principles: OOAD is grounded in object-oriented principles, such as encapsulation, inheritance, and polymorphism. These principles promote code organization, maintainability, and extensibility. By adhering to object-oriented principles, the Self-Sovereign Identity Verification System can be designed with well-defined classes and objects, allowing for easy modification, extension, and adaptation to changing business needs.
4. Security and Privacy Considerations: The OOAD methodology allows for the integration of security and privacy considerations throughout the system's design and development.

By employing design patterns and incorporating security measures from the early stages, the Self-Sovereign Identity Verification System can address vulnerabilities, protect sensitive data, and ensure compliance with privacy regulations.

5. Iterative and Incremental Development: OOAD promotes an iterative and incremental development approach, allowing for the system to evolve and improve over time. This approach enables the project to deliver functional components in incremental stages, gather feedback, and incorporate changes based on user requirements and emerging technologies. Fostering flexibility and adaptability.

3.4 Development Tools

The development of the Self-Sovereign Identity Verification System will utilize a combination of tools and technologies to facilitate efficient implementation. The specific tools and technologies include:

1. Programming Languages: The system will be developed using languages such as JavaScript, Python, and Java.
2. Frameworks and Libraries: Frameworks like Hyperledger Indy, Hyperledger Aries and Sovrin will be leveraged to implement the SSI functionality. Additionally, relevant libraries and SDKs specific to the chosen frameworks will be utilized.
3. Integrated Development Environment (IDE): An IDE such as Visual Studio Code
4. Version Control System (VCS): GitHub will be utilized to host the Git repositories and facilitate efficient code management.

CHAPTER 4: SYSTEM ANALYSIS AND DESIGN

Use Case Descriptions:

- Initiate Identity Verification: The user initiates the identity verification process by providing the required personal information and consent to the Self-Sovereign Identity System.

- Verifies Identity: The Self-Sovereign Identity System verifies the user's identity using the provided information, encrypted data, and blockchain-based validation mechanisms.

- Manages Identity: The user can manage their digital identity within the Self-Sovereign Identity System, including updating personal information, controlling data sharing permissions, and managing verifiable credentials.

References

Abraham, A. (2022). *Qualified Self-Sovereign Identity: Addressing the gaps between Self-Sovereign Identity and traditional Identity Systems* [PhD Thesis]. https://doi.org/10.13140/RG.2.2.29266.22728

Allen, C. (n.d.). Life With Alacrity. *The Path to Self-Sovereign Identity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Garg, S., & Vashisht, R. (2021). A Permissioned Blockchain System for Secure Multiparty Computation. *Journal of Physics: Conference Series*, *1998*, 012003. https://doi.org/10.1088/1742-6596/1998/1/012003

Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review*, *10*. https://doi.org/10.14763/2021.2.1550

Jamal, A., Helmi, R., Syahirah, A., & Fatima, M.-A. (2019). *Blockchain-Based Identity Verification System*. 253–257. https://doi.org/10.1109/ICSEngT.2019.8906403

Jena, S., & Barik, R. C. (2023). *Decentralized Digital Identity: A New Form of Secured Identity Using Blockchain Technology* (pp. 93–102). https://doi.org/10.1007/978-3-031-31153-6_9

Microsoft. (n.d.). *Microsoft Decentralized Identity*. https://go.microsoft.com/fwlink/?linkid=2216241&clcid=0x409&culture=en-us&country=us

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://www.bitcoin.org/bitcoin.pdf

Oxford English dictionary (Online). (n.d.). Oxford University Press.

UPort. (n.d.). https://www.uport.me/

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.8202