TITLE:

DECENTRALIZED IDENTITY VERIFICATION

A Project work completed in partial fulfilment of the requirements

For

Certificate in Web 3 Development

BY:

GLORIA DEDE TETTEH 0207049336

SEPTEMBER,2023

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

Identity verification is the process of proving that an entity is who or what it claims to be. In an increasingly digital world, the need for secure and reliable identity verification has never been more critical. Traditional methods often fall short, exposing individuals to privacy risks and leaving organizations susceptible to fraud. This proposal outlines a groundbreaking project that aims to address these challenges through the implementation of a decentralized identity verification platform. Some of these challenges include:

- Privacy: Centralized intermediaries can collect, store, and sell personal data without the consent or knowledge of the users.
- Security: Centralized intermediaries can be hacked, compromised, or corrupted, leading to identity theft, fraud, or misuse of personal data.
- Inclusion: Centralized intermediaries can exclude or discriminate against certain users based on their location, nationality, or other criteria.
- Portability: Centralized intermediaries can lock users into their platforms or services, preventing them from switching or accessing other providers.

By harnessing the power of blockchain technology, we envision a solution that not only provides a secure means of verifying identities but also ensures privacy and data integrity at every step. This platform will leverage the ERC725/ERC735 identity standards, which have emerged as a leading framework for decentralized identity management on the Ethereum blockchain.

This proposal outlines the objectives, scope of work, timeline, and budget for the development of this innovative decentralized identity verification platform. Our team is committed to creating a solution that not only meets industry standards but sets a new benchmark for secure and privacy-centric identity verification.

We believe that this project has the potential to revolutionize the way identities are verified in the digital realm, offering individuals and organizations a seamless, trustworthy, and privacy-preserving solution. We look forward to embarking on this journey and contributing to the advancement of digital identity technology.

1.2 PROBLEM STATEMENT

This project outlines a groundbreaking project that aims to address these challenges through the implementation of a decentralized identity verification platform. Some of these challenges include:

- Privacy: Centralized intermediaries can collect, store, and sell personal data without the consent or knowledge of the users.

- Security: Centralized intermediaries can be hacked, compromised, or corrupted, leading to identity theft, fraud, or misuse of personal data.

- Inclusion: Centralized intermediaries can exclude or discriminate against certain users based on their location, nationality, or other criteria.

- Portability: Centralized intermediaries can lock users into their platforms or services, preventing them from switching or accessing other providers.

1.3 AIMS AND OBJECTIVES

AIMS

To address these challenges, we propose a solution for decentralized identity verification using blockchain technology. Blockchain can provide the following benefits for identity verification:

- Privacy: Users can control their own identity data and decide who can access it and for what purpose.
- Security: Users can use cryptographic keys to sign and verify their identity data, making it tamper-proof and verifiable.
- Inclusion: Users can access any service or platform that supports the decentralized identity standard, regardless of their location or background.
- Portability: Users can take their identity data with them across different services or platforms, without losing their history or reputation.

OBJECTIVES:

- Create a Secure Identity Verification System: Develop a robust and tamper-proof system for verifying identities while prioritizing user privacy and security.
- Utilize Blockchain Technology: Leverage the Ethereum blockchain and ERC725/ERC735 identity standards to establish a decentralized and immutable identity verification process.
- Ensure Privacy-Preserving Solutions: Implement cryptographic techniques to protect sensitive user information and enable selective disclosure of identity attributes.
- Enable Interoperability: Design the system to be compatible with existing identity verification standards and systems, facilitating integration with external services and platforms.
- Compliance and Regulatory Considerations: Ensure adherence to relevant data protection and privacy regulations, such as GDPR, to maintain legal compliance.

1.4 SOLUTION OVERVIEW

This solution is based on the ERC725/ERC735 identity standards proposed by Fabian Vogelsteller1, the creator of ERC20 and Web3.js. ERC725 is a standard for publishing and managing an identity via a smart contract on the Ethereum blockchain. ERC735 is an associated standard for adding and removing claims to an ERC725 identity smart contract. These standards enable the following features:

- Self-sovereign identity: Users can create and own their own identity smart contracts, without relying on any central authority or intermediary.
- Multi-key management: Users can use multiple keys to control their identity smart contracts, allowing for different levels of access and delegation.
- Proxy functionality: Users can use their identity smart contracts to interact with other smart contracts or DApps on the blockchain, acting as a proxy for their actions.
- Verifiable claims: Users can add and remove claims to their identity smart contracts, which are attestations made by third parties or themselves about their attributes or capabilities.

1.5 SCOPE OF WORK

Phase 1: Planning and Research:

- Conduct in-depth research on existing identity verification solutions, blockchain-based identity standards, and legal frameworks surrounding identity verification.
- Define specific user stories, use cases, and personas to guide development.
- Develop a detailed technical architecture for the decentralized identity verification platform.

Phase 2: Smart Contract Development

- Implement smart contracts utilizing ERC725/ERC735 identity standards for creating, managing, and verifying identities.
- Establish a mechanism for users to securely associate identity attributes with their Ethereum address.

Phase 3: User Interface Development

- Design an intuitive and user-friendly interface for identity creation, verification requests, and attribute sharing.

- Ensure compatibility with various devices and browsers to maximize accessibility.

Phase 4: Privacy and Security Measures

- Implement cryptographic protocols to protect user data during identity verification and attribute sharing processes.

- Conduct rigorous security testing and auditing to identify and address vulnerabilities.

Phase 5: Integration and Testing

- Integrate the decentralized identity verification platform with external services, if applicable.

- Conduct comprehensive testing, including unit testing, integration testing, and user acceptance testing.

Phase 6: Documentation and Compliance

- Create comprehensive documentation including user guides, developer documentation, and compliance statements.

- Ensure compliance with relevant data protection regulations and standards.

CONCLUSION

This project aims to revolutionize identity verification by leveraging blockchain technology and ERC725/ERC735 identity standards. By prioritizing security, privacy, and compliance, we aim to deliver a solution that sets a new standard for decentralized identity verification.