SCAR: A *blockchain* based approach for academic registry

Projeto e Seminário

Licenciatura em Engenharia Informática e Computadores

Diogo Rodrigues

Gonçalo Frutuoso

49513@alunos.isel.pt

49495@alunos.isel.pt

Orientadores

Cátia Vaz

Alexandre Francisco

cvaz@cc.isel.ipl.pt

aplf@tecnico.pt

May 14, 2024

Abstract

This is the abstract.

Resumo

Aqui fica o resumo.

Acknowledgments

Here goes the acknowledgments.

Índice

List of Figures

List of Tables

Chapter 1

Introduction

This is where the introduction goes to.

1.1 Outline

This is where the outline goes to. The outline is a guide for the reader to understand the structure of the document.

Chapter 2

Background

2.1 Introduction to the Problem

In today's fast paced world, the authenticity and accessibility of academic certificates play a crucial role in ensuring trust and credibility in various domains, ranging from education to employment and beyond. The current and traditional *paper-based* system of issuing and verifying academic certificates is not only time consuming but also prone to a lot of fraud and manipulation. The rampant proliferation of counterfeit certificates, inefficient verification processes and the risk of loss or damage highlight the need for a more reliable, robust and secure academic certificate registry system.

The current system of academic certificate registry is plagued by numerous challenges. Firstly, the reliance and trust on paper-based certificates is a major issue making them susceptible to forgery and tampering undermining the cridibility and integrity of academic qualifications. Secondly, the manual verification process is time-consuming and prone to errors, leading to delays in credential validation, possible fraudulent activities and also potential loss of revenue for institutions due to errors in the manual release. Thirdly, the centralized nature of certificate issuance by educational intituitions exacerbates the difficulty of maintaining a unified and updated registry, hampering efficient verification mechanisms.

2.2 Alternative Approaches

Several attemps have been made to address the imperfections of the traditional academic certificate registry system. One such solution is the implementation of *centralized databases* [1] managed by government or regulatory authorities, where educational institutions are required to submit digital copies of certificates for verification purposes. Additionally this approach aims to centralize certificate records and simplify the verification process, it still faces challenges such as the risk and concerns of data privacy and security, interoperability issues between different databases and the need of a trusted third party to manage the database. This centralized mechanism of keeping record is also devoted to have a single point of failure.

Another solution that is gaining traction is the adoption of *blockchain technology* for academic certificate registry. Blockchain offers a decentralized, secure and tamper-proof ledger where certificates can be stored and verified. The use of blockchain technology ensures that certificates are immutable, transparent and accessible to all stakeholders. Moreover, this technology enables the instant verification trough cryptographic methods, eliminating the need for a central authority to manage the registry, thereby reducing the risk of fraud and manipulation. This approach eliminates the need for a central authority to manage the registry, thereby reducing the risk of fraud and manipulation.

In contrast to the traditional centralized databased system, in our opinion, blockchain emerges as a disruptive force capable of revolutionizing academic certificate registry systems by providing in a decentralized and secure manner, an immutable and tamper-proof ledger where certificates will be stored and verified. The decision to embrace blockchain technology as the foundation of our solution is based on what we sad above as well as the fact that blockchain technology is a key enabler of the *Web3* vision, which aims to create decentralized applications (dApps) that are secure, transparent and trustless where users have full control over their data and digital assets without having a **single point of failure**.

2.3 Blockchain

2.4 Differente Approaches to Blockchain

Chapter 3

Requirements

This is where the requierments go to.

3.1 Smart Contracts

Chapter 4

Solution Architecture

This is where the architecture goes to.

4.1 Multiplatform Application

This is where the multiplatform application goes to. Some descrpition what it is, how it works, which solutions are available and detailed talk about the chosen one.

Chapter 5

Implementation

This is where the implementation goes to.

Chapter 6

Work Plan

This chapter describes the work plan for the project.

Bibliography

[1] J. E. Olson. Chapter 5 - origins of a database archiving application. In J. E. Olson, editor, *Database Archiving*, The MK/OMG Press, pages 71–84. Morgan Kaufmann, Boston, 2009.