SCAR: A *blockchain* based approach for academic registry

Projeto e Seminário

Licenciatura em Engenharia Informática e Computadores

Diogo Rodrigues
49513@alunos.isel.pt

Gonçalo Frutuoso
49495@alunos.isel.pt

Orientadores

Cátia Vaz
cvaz@cc.isel.ipl.pt

Alexandre Francisco
aplf@tecnico.pt

May 15, 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* [4] 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 Distributed System

As we transition to a blockchain-based solution for our problem it is crucial to understand the foundational concepts that make this technology both revolutionary and reliable. Central to blockchain's efficacy is the principle of *distributed consensus*, which ensures the integrity, security and transparency of the ledger. This next sections explore into the mechanics of distributed consensus, the broader vision of *Web3* and other key concepts integral to understanding how blockchain can trasnform academic certificate registry systems.

Blockchain Technology

Blockchain is a technology behind the cryptocurrency Bitcoin initially described by Satoshi Nakamoto in a 2008 white paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' [3]. Although the term blockchain gained popularity in that year, with the introduction of Bitcoin cryptocurrency by Nakamoto, its underlying concepts have been used since the 1980s. Later in 2004, Harold Thomas Finney II (Hal Finney) introduced the Reusable Proof of Work (*RPOW*) system [2]. The RPOW system was a digital currency system that used a *proof-of-work* limit the amount of work done by the server and to limit the amount of work done by the client. The RPOW system was the first system to use a blockchain-like structure to store and verify transactions. After sometime, in 2009 the first bitcoin transaction was made by Nakamoto to his friend Hal Finney [5] where was tranfered 10 BTC (bitcoin). This marked the beginning of the blockchain technology era. In 2013, Vitalik Buterin proposed the concept of *smart contracts* in his white paper 'Ethereum: The Ultimate Smart Contract and Decentralized Application Platform' [1]. Uppon this publication, *Ethereum* has launched his own blockchain in 2015. [6].

All of the above information is to show how blockchain has evolved over the past few years and is presented in [7].

What is Blockchain?

A blockchain is a time-ordered set of blocks where each block is cryptographically linked to the previous one forming a chain. All blocks are stored in a decentralized and distributed ledger and become thrustworthy digital records whar are unmodifiable in practice but very easy to verify. Like mencioned in the previous section 2.2 there is no centralized or hierarchical structure in the blockchain network and the information is shared by a network of *peers*.

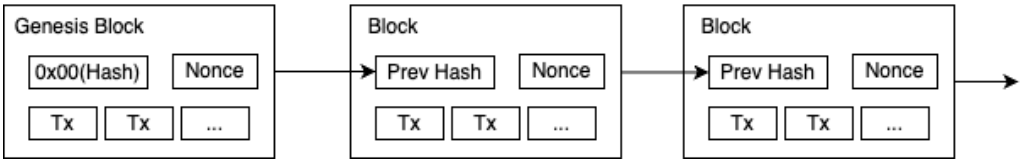

Figure 2.1: Blockchain structure adapted from [3]

Each block contains a reliable register of one or more actually executed transactions that are created and exchanged by the network participants (peers) which eventually must modify its state. To add new information to the chain, a **consensus** about its truthfulness must be reached among the peers in the network.

The content of each transaction that is stored in a single block depends on the specific type of blockchain and its prupose. In our case and very succinctly, the transaction has an 'item' that contains information about the academic certificate; we will discuss this in more detail in the next chapters. Other example used for the time being is the Bitcoin, where the main information registered are exchanges of bitcoins between accounts.

Other important aspect of the chain and the major reason for its security is the **hash**. The hash is a mathematical function that takes an input (or 'message') and returns a fixed-size string of bytes. This function is used to verify whether or not the data contained in the block has been tampered with. It is created when a new block is added or updated on the chain. Any minimal change in the block's content will result in a completely different hash, also the hash of a block contains the information of the previous block's hash. This is the reason why the blockchain is considered tamper-proof and secure.

Distributed Consensus Mechanisms

Distributed consensus feature allows a blockchain-based system

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] V. Buterin. Ethereum: the ultimate smart contract and decentralized application platform. *Libro blanco de Ethereum. Available at: http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html* , 8, 2013.

[2] H. Finney. Rpow-reusable proofs of work. Available at: `https://nakamotoinstitute.org/finney/rpow/index.html`, 2004.

[3] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Available at SSRN: https://ssrn.com/abstract=3440802 or http://dx.doi.org/10.2139/ssrn.3440802*, August 2008.

[4] 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.

[5] A. Peterson. Hal finney received the first bitcoin transaction. here's how he describes it. *Washington Post, available at: https://www.washingtonpost.com/news/the-switch/wp/2014/01/03/hal-finney-received-the-first-bitcoin-transaction-heres-how-he-describes-it/*, 3, 2014.

[6] N. Reiff. Bitcoin vs. ethereum: what's the difference. *Investopedia, available at: https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp* , 2020.

[7] G. Tripathi, M. A. Ahad, and G. Casalino. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, 9:100344, 2023.