Principles of Information Security

DECENTRALIZED SYSTEM FOR CERTIFICATE VERIFICATION

Project Proposal

AadilMehdi Sanchawala Adhithya Arun Meher Shashwat Nigam (PoC)
Rohan Chacko Sumaid Syed

Problem

In the traditional degree certificate system, employers need to trust intermediaries eg. certificate holders, teachers, and university officials for the legitimacy of certificates and documents. This has resulted in a sharp rise of fraudulent activities by intermediaries to produce fake diplomas or degree certificates. Additionally, certificates and other personal information are usually stored in a centralized server or data warehouse which is prone to tampering or hacking. Existing solutions to this problem face many issues with respect to authentication, authorization, confidentiality, privacy, and ownership.

Proposed Solution

The need for a decentralized solution is evident in this use-case. Blockchain technology, a common decentralized solution, is revolutionary for its potential to build systems where strangers can transact with each other without the need of any intermediary to oversee the transaction between the parties thus reducing fraudulent activities and data tampering. Blockchain provides features such as decentralization, transparency, and tamper-proof data-storage which replaces the need for trust on intermediaries for verifiable certification.

Our solution consists of a web application built on top of a blockchain network. Trusted education providers issue official certificates to students and/or working professionals as a proof of completion or achievement. The trusted providers are required to upload these official certificates using the application onto the blockchain network. The corresponding certificate for each student and/or professional is linked to their profile on the app. Any trusted company looking to hire potential candidates can use this application to have a verifiable history of an applicant's educational qualifications. Since the blockchain network is immutable and each transaction on the network is time-stamped, the hiring company can be sure that all qualifications linked to a particular candidate's profile are from trusted sources.

The proposed framework could also provide the corresponding functions for post-university education and even for online courses, that are rapidly gaining popularity. Conceptually, this solution is scalable for any legal document verification systems.

Implementation Details

There are various blockchain platforms available such as Ethereum, Hyperledger Fabric, Besu, etc. Ethereum is a permissionless blockchain, where anyone can join the network as well as write and read transactions. On the other hand, Hyperledger Fabric is a permissioned blockchain, where only predefined participants can join a network, view and make transactions; hence seems like the right choice.

We intend to use a pre-existing blockchain solution like Hyperledger Fabric or Ganache that enables us to create a private blockchain network. We will build a web application on top of this network to allow educational institutions to upload original documents and employers to inspect validity of required documents.

Goals

1. **Research** and explore various architectures/frameworks to enable verifiable storage of educational history of students and/or working professionals to aid employers in the hiring process.
2. **Development** of a decentralised web application to store & verify educational history of students based on a blockchain network
3. **Test** the application with a local blockchain network consisting of multiple users as a proof of concept.

Milestones

1. Weeks 1 - 2

   Explore previous research and understand the literature in the same domain

2. Weeks 3 - 4

   Build a high level design and architecture of the solution

3. Weeks 5 - 6

   Think of low level design and various implementation strategies

4. Weeks 7 - 8

   Implement the contracts and web app

5. Weeks 9 - 10

   Finish development

Division of work

Exact roles yet to be decided. Blockchain network and web application development will be equally distributed between team members.