CertNet

DECENTRALIZED SYSTEM FOR CERTIFICATE VERIFICATION

Team 11

AadilMehdi Sanchawala
Adhithya Arun
Meher Shashwat Nigam
Rohan Chacko
Sumaid Syed

The problem

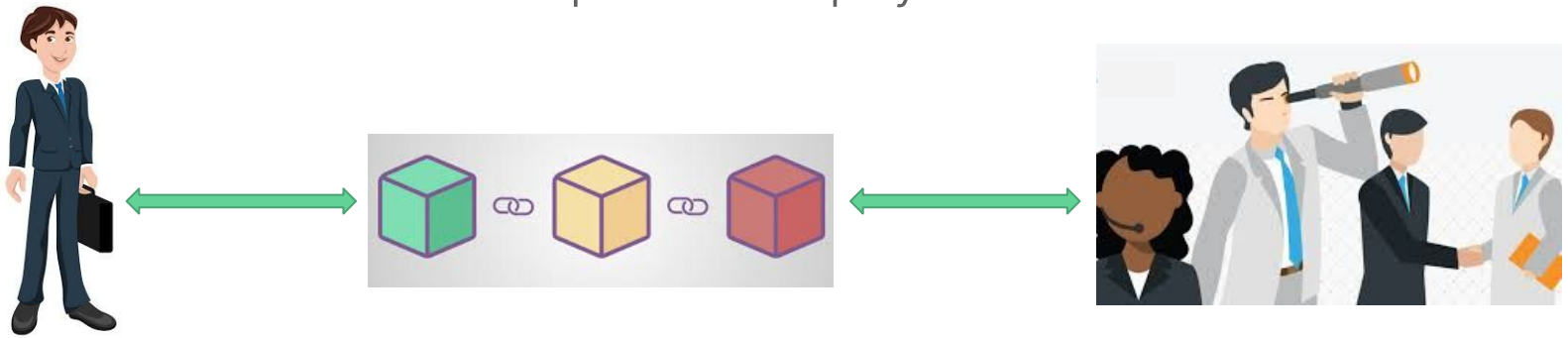
Employers need to trust intermediaries eg. certificate holders, teachers, and university officials for the legitimacy of certificates and documents.

- This has resulted in a sharp rise in **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**.
- There is a lot of **time and effort wasted** on employee educational records verification. This takes around 4-5 days[1] on an average for each potential employee.

[1] https://www.hireright.com/blog/background-checks/how-long-does-an-employee-background-check-take

The solution: CertNet

Our main objective is to create a **decentralized certificate verification system built on blockchain**, allowing employers to verify certifications of their potential employees.



But, Why Blockchain?

A distributed credential management system built over a blockchain network has many advantages over the prevalent centralized, federated, or distributed systems.

Why Blockchain?

- **Decentralization**
  Ownership and control over data are not centralized by a single governing body on the blockchain.
- **Immutability and Persistence**
  Immutable records of all historical activities are maintained in an append-only *distributed ledger* of the blockchain guaranteeing that the system is tamper-resistant.
- **Transparency**
  Every participant is aware of all activities and changes to the recorded data since every valid exchange, committed as a transaction, is accessible and explorable to all the participants in the network.
- **Trustlessness**
  The participants of the network do not necessarily know each other or who they can trust.

Why Blockchain?

- **Distributed and Shared**
  Data present in the distributed ledger is shared with everyone in the network. This removes the need for replication of data making the system cost-efficient.
- **Anonymity**
  The participants of the network do not reveal their actual identity. Instead, they use their cryptographically generated public addresses as pseudonyms.
- **Consensus**
  A new block is created only on the basis of some consensus mechanism such as (but not limited to) Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance (PBFT), Proof-of-Elapsed Time (PoET), etc., which helps establish trust required for verifying and validating data in a trust-less environment.

Use Case and Target Audience

Use case

Our primary use-case is in the domain of **industry hiring**. Job portals such as *Joveo* and *Indeed* have found success in matching the right applicant for a company's job description. But there is still the issue of **verifying candidate credentials**.

Our product would fill this gap by introducing a web-based application that stores and verifies each certificate and/or document associated with a person. An employer looking to hire a candidate can then verify a potential employee's certificates using our application.

Target audience

Currently, our target audience are **recruiters and HR teams** or any company that conducts the hiring process manually, and **students/professionals.**

Related work

Blockcerts

Blockcerts provides an open standard and is a project that aims to build a system for creating, sharing, and verifying blockchain-based educational certificates.

CertChain

CertChain is a blockchain-based public and efficient audit scheme for TLS connections.

Open Badges

Open Badges is the world's leading standard for digital badges. Open Badges is not a specific product or platform, but a type of digital badge that is verifiable, portable, and packed with information about skills and achievements.

What’s the current progress?
What have we done?

Application Architecture

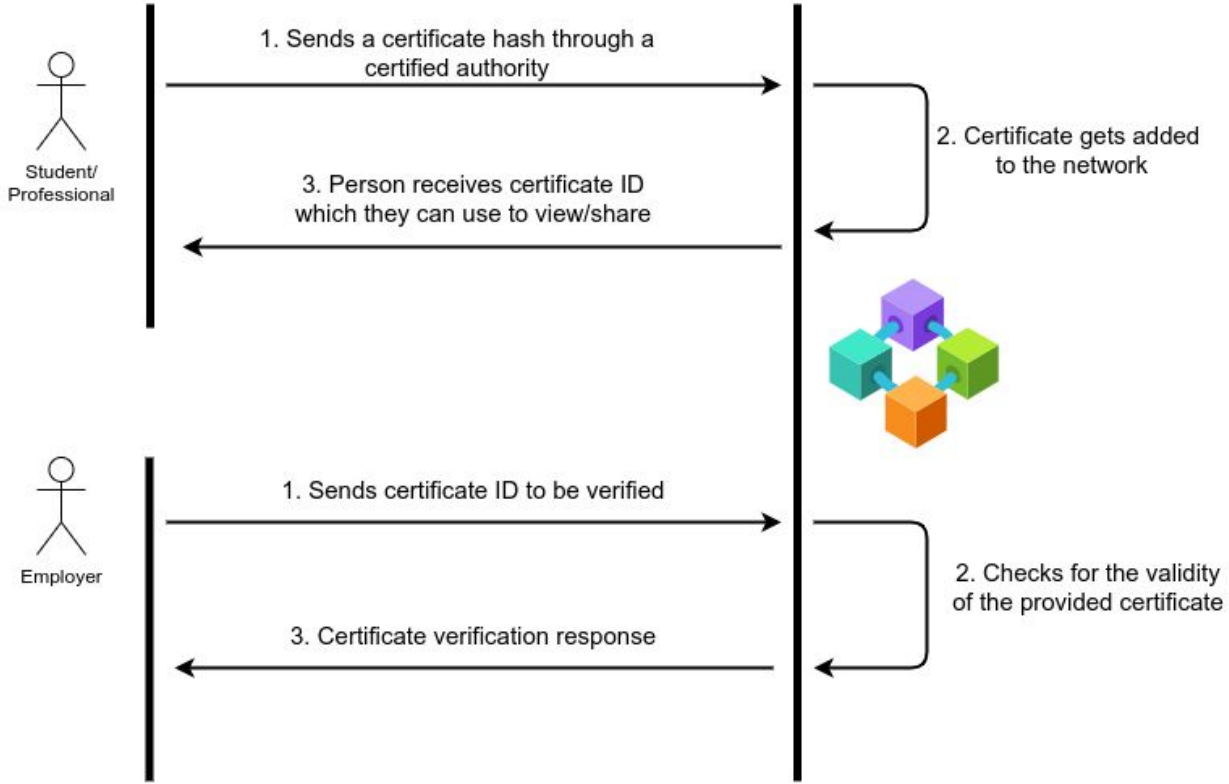
- We are following a **microservice architecture** for the overall design of the application. Each component of the application will be a seperate microservice **containerized** inside docker and hosted independently.

- A microservice architecture makes it easy to develop applications based on a distributed system and provides **high scalability and fault tolerance**.

- We are following a **modular structure** for scalability and extensibility.

- We are following **test-driven development** and writing unit tests for each module after it's implemented.

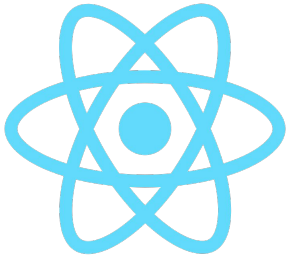
How does it work?



Frameworks

After much deliberation we chose the following:

- Local Network : *Ganache*
- Backend : *Express*
- Frontend : *React*
- Database : *MongoDB*



Why Ganache?

- Open source
- Supports local blockchain networks for development
- Modular architecture
- Ease of development of DApp
- Can be deployed on any network

Implementation so far

1. Local setup of Ganache
2. Truffle configuration setup
3. Database and Express server setup
4. Certificate generation HTTP request and smart contract
5. UI for certificate generation

The road ahead...

Features

- User login authentication
- User profile with a list of associated verified certificates
- Display a certificate given a certificate hash (for professionals)
- Verify a certificate given a certificate hash (for employers)

Testing

- Unit tests for each component and a final integration test after integrating all components

Possible extension

Our application can be extended to be a job search engine. Since we already provide document verification, recruiters can easily trust the recommendations we come up with. An additional step of an optimal matching algorithm should be developed.

Since the participants (certificate holders) in the network are anonymous, the company can reach out to relevant profiles. This removes bias as well.

Once people receive the notification about the interest of any recruiter, they may choose to apply to the company.

App Demo