



CERTNET

DECENTRALIZED SYSTEM FOR CERTIFICATE VERIFICATION

Aadil Mehdi Sanchawala

Adhithya Arun

Sumaid Syed

Meher Shashwat Nigam

Rohan Chacko

Team 11

PROBLEM

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



PROBLEM



Sharp rise in fraudulent activities by intermediaries to produce fake diplomas or degree certificates.

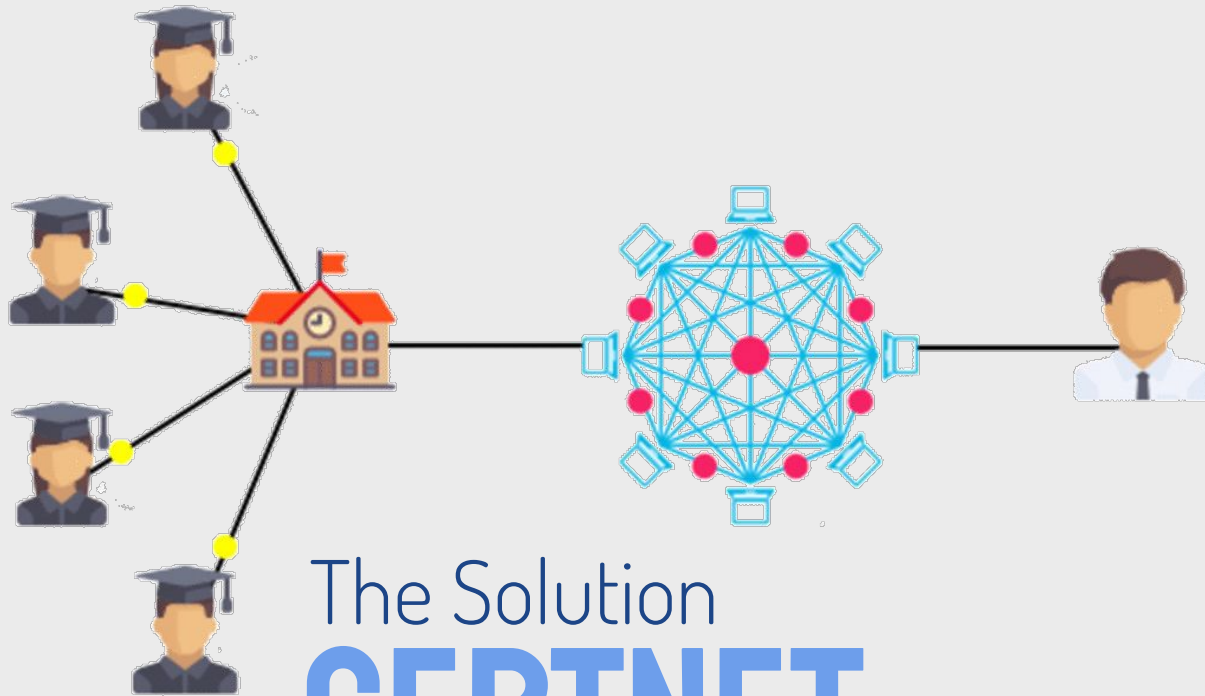


Certificates and other personal information are usually stored in a centralized server or data warehouse which is prone to tampering or hacking.



Wasted time and effort on employee educational records verification. Takes around 4-5 days^[1] on an average for each potential employee.

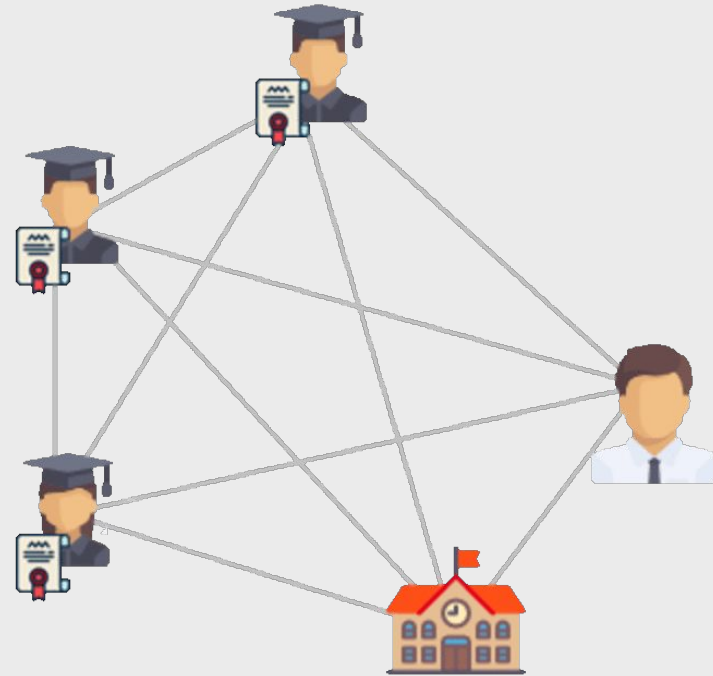
[1] <https://www.hireright.com/blog/background-checks/how-long-does-an-employee-background-check-take>



The Solution
CERTNET

CERTNET

Create a **decentralized certificate verification system** built on **blockchain**, allowing employers to verify certifications of their potential employees.



WHY BLOCKCHAIN?

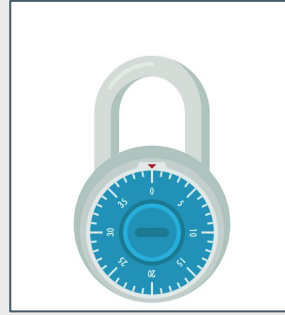
A DISTRIBUTED CREDENTIAL MANAGEMENT SYSTEM BUILT OVER A BLOCKCHAIN NETWORK HAS MANY ADVANTAGES OVER THE PREVALENT CENTRALIZED, FEDERATED, OR DISTRIBUTED SYSTEMS.

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

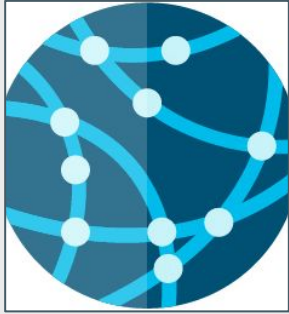
Every participant is aware of all activities and changes to the recorded data. Each transaction is accessible and explorable to all the participants in the network.



TRUSTLESSNESS

The participants of the network do not necessarily know each other or who they can trust.

WHY BLOCKCHAIN?



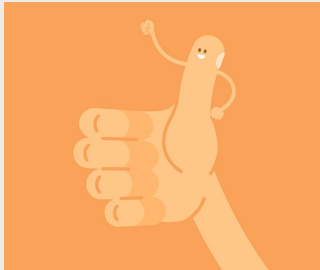
DISTRIBUTED AND SHARED

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

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.



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 & TARGET AUDIENCE

JOB PORTALS

VERIFYING CANDIDATE CREDENTIALS

RECRUITERS AND HR TEAMS

STUDENTS & PROFESSIONALS



RELATED WORKS



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.



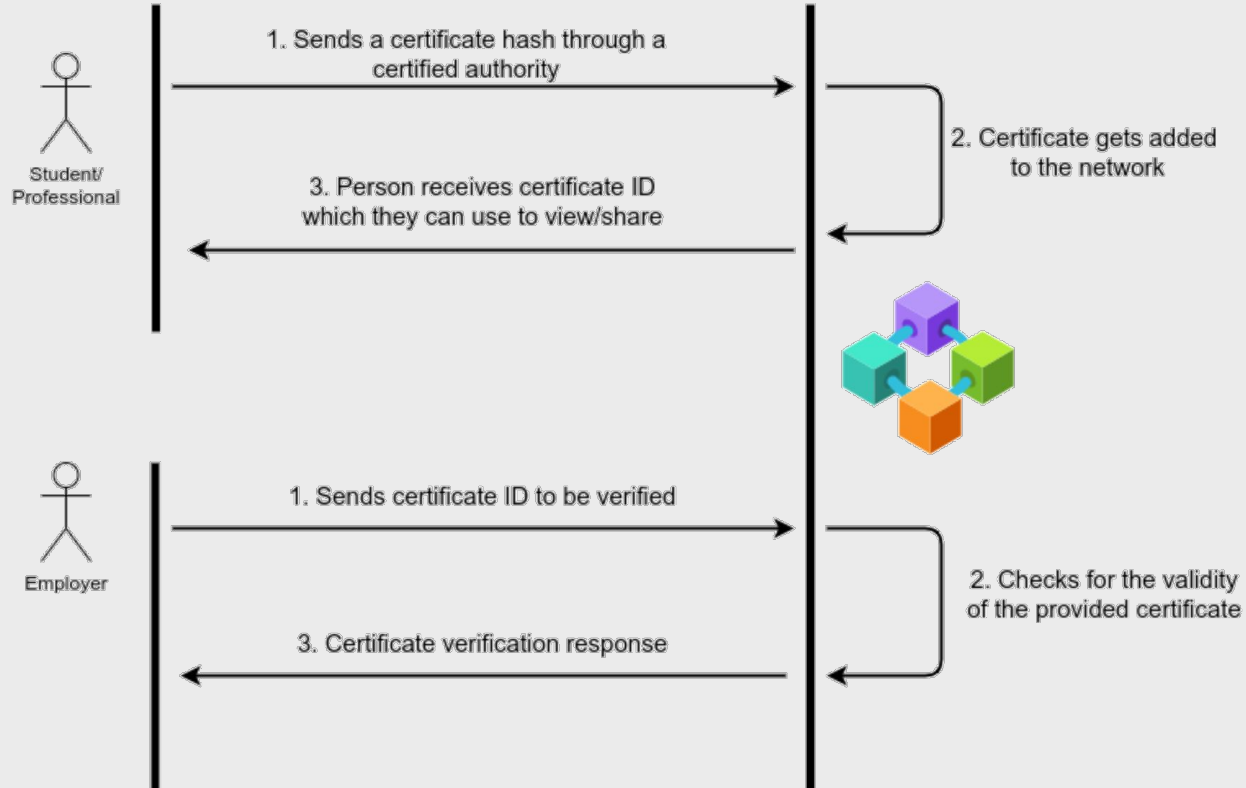
DESIGN

APPLICATION ARCHITECTURE



- We are following a **microservice architecture** for the overall design of the application. Each component of the application will be a separate 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.

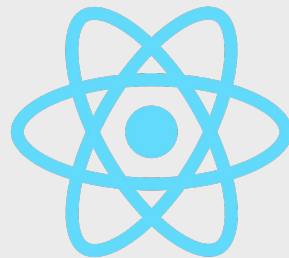
HOW DOES IT WORK?



FRAMEWORKS

Our implementation uses the following:

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



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







[illegible]



PHASE I



TARGETS ACHIEVED






-  Understand blockchain and its use-cases
-  Experiment using Web3, React, Solidity & other tech required for DApp development
-  Creating the smart contract for our app in Solidity
-  Creating the React App using Express.js as backend and MongoDB as database
-  Local setup of Ganache
-  Truffle configuration setup



PHASE II








TARGETS ACHIEVED

-  Database and Express server setup
-  Certificate generation HTTP request and smart contract
-  UI for certificate generation
-  Authentication with two types of users - Organization and Student
-  Generate user profiles using Google accounts



TARGETS ACHIEVED

-  UI for viewing list of certificates
-  Certificates issued by an organizations
-  Certificates issued to a student
-  Certificate verification to ensure against certificate tampering and illegal insertion in DB
-  Unit Tests for each component of the DApp

APP ORCHESTRATION & STAKEHOLDERS



ORGANIZATION VIEW

- Register as a user of type “Organization”
- Generate certificates for a particular Degree for a particular duration
- Certificates are only issued for the students with an associated account on the network
- Verify certificates issued to students
- View the list of certificates issued by the organization
- Only authorized organizations can take part in the blockchain network
- Public URL of certificate will show the associated student and organization, this will prevent "fake" students claiming certificate to be theirs

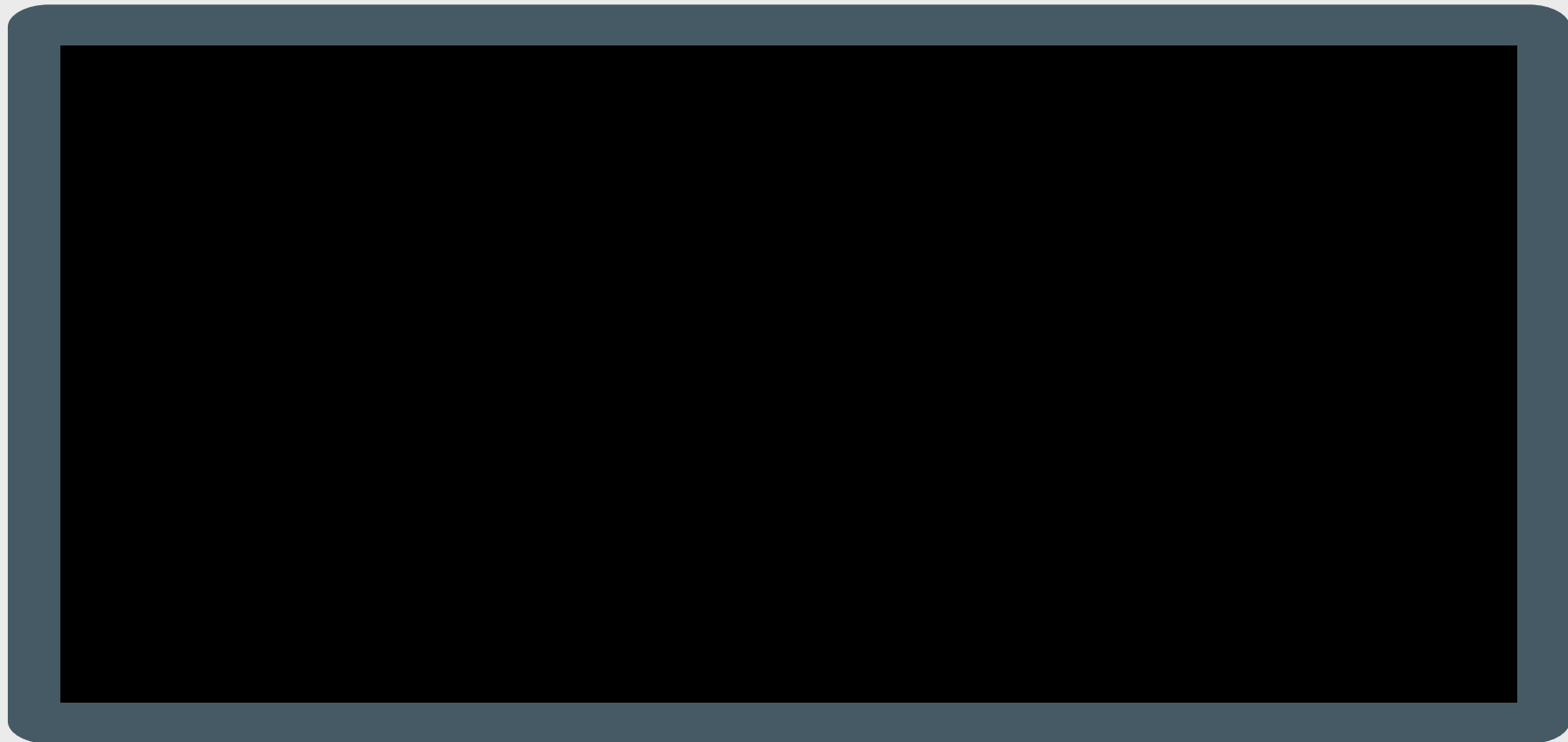
STUDENT VIEW

- Register as a user of type “Student”
- View list of certificates issued to them
- View and verify certificates issued to them
- Organizations can't tamper with students' data without student knowing
- If certificate is “fake” i.e. certificate is maliciously added to the database or if an existing certificate is tampered, the certificate will show unverified.
- Student can generate the public url to certificate which can be used by employers to verify the certificate

BLOCKCHAIN VIEW

- The smart contract is deployed as a transaction on the blockchain. The contract gets a unique address which can be used to identify it.
- The students and organizations interact with the smart contract using the public functions of the smart contract that is exposed to them.
- For simplicity, we abstract the endpoints of the smart contract by mapping user interactions with the app to corresponding calls to appropriate functions in the contract
- Each of these interactions with the contract are recorded as transactions in blocks on the blockchain and can be viewed on Ganache.
- Each certificate is a transaction between an organization and a student, where both have a unique identity (address) on the network.

APP DEMO



POST-COURSE SCOPE

- **Features**

- Authentication using other methods such as GitHub, Facebook, etc.
- Ability to search through different students using name
- Ability to filter certificates by students, date, degree, etc

- **Deployment**

- Deploy the app on a public network

- **UI**

- Make UI responsive for any device layout

- **Error Handling**

- Verification of courses for which an organization can issue certificates



THANK YOU

