Digital Certificates using Blockchain

By: Alley Mostafa, Sherif Abdel Khalek, Mohamed Reda, Shehab El-Din Mohamed

Supervised by: Dr. Ayman Nabil,

Eng. Radwa Samy

Introduction (1/3)

- 94% of the forged certificates in Kuwait were Egyptian in 2018.
- 44 of the 47 fraud certificate cases were Egyptian universities.

Introduction (2/3)

What is Blockchain?

Characteristics of Blockchain:

- Consensus
- Provenance
- Immutability
- Finality

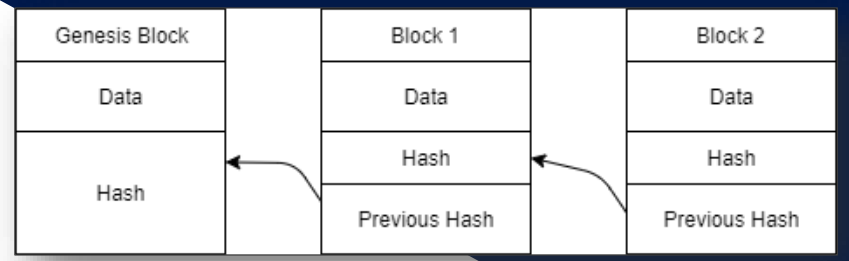
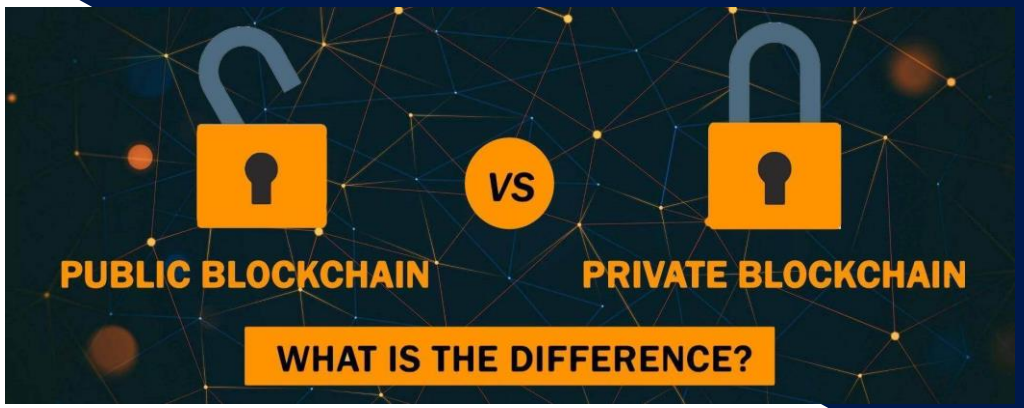


Figure 1: Blockchain

Introduction (3/3)

Types of Blockchain:

- Public
- Private
- Permissioned



Ethereum vs Fabric vs Indy

	Ethereum	Hyperledger fabric	Hyperledger indy
Purpose	For business and generalized application	General purpose and high flexibility of permissions	built for decentralized identity
Confidentiality	Transparent	Private and confidential	approach to privacy
Mode of Peer Participation	Permissionless, Public or Private	Permissioned, Private	Permissioned, Public
Consensus Mechanism	Proof-of-Work algorithm	No mining required	No mining required
Smart contract	Smart Contract written in (e.g., Solidity)	Smart Contract written in (e.g., Go, JavaScript (Node.js))	Not supporting any smart contract
Cryptocurrency	Cryptocurrency called ether	No built-in cryptocurrency	No built-in cryptocurrency
Governance	Ethereum developers	Linux Foundation	Linux Foundation

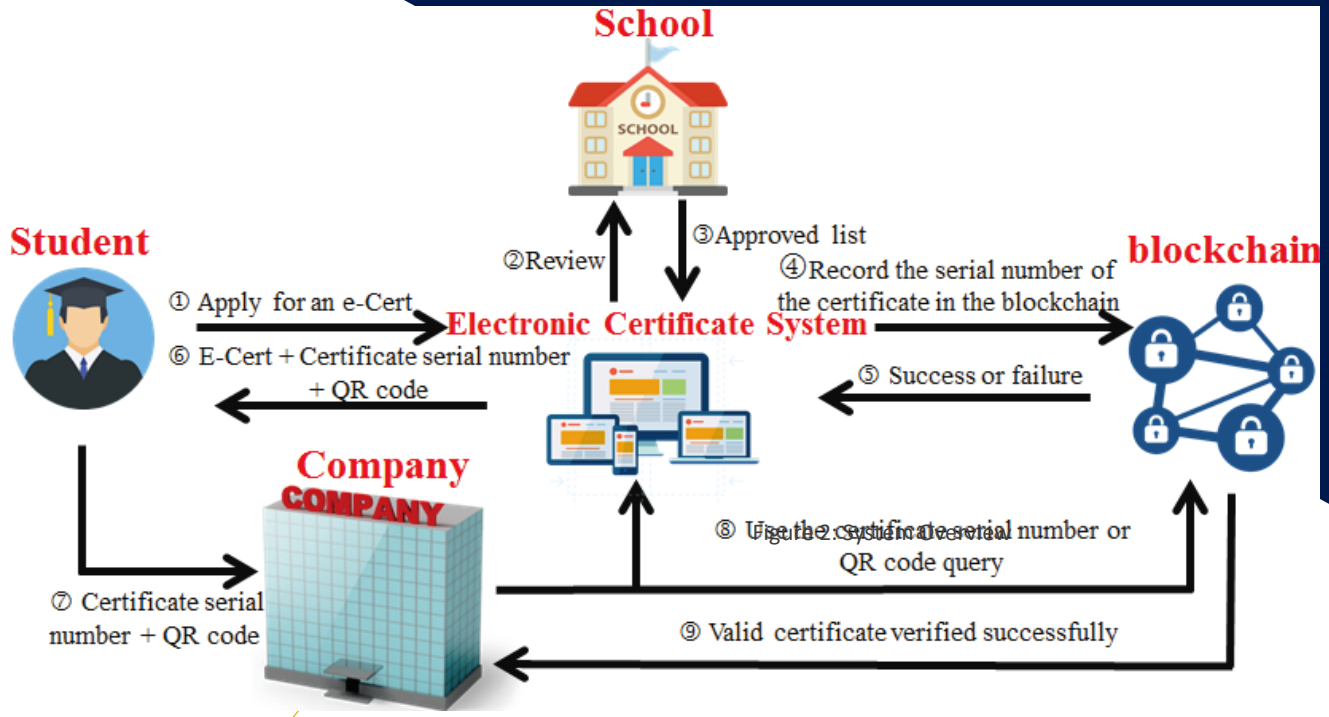
Motivation

- The need for such system to the Egyptian educational system to prevent forgery.
- It’s inspired by previous projects such as MIT’s Blockcerts.

Related Work (1/3)

Blockchain and Smart Contract for Digital Certificates. (2018)

- Technologies used:
  - Ethereum Virtual Machine.
  - Solidity
  - Smart Contracts
- Outcome:
  - An Electronic-Certificate.
  - QR code and Serial Number.
  - Data recorded on the Blockchain



Related Work (2/3)

CVSS: A Blockchainized Certificate Verifying Support System. (2018)

- The system provides:
  - An e-cert .cvss file includes:
    - Hash value.
    - Blockchain information (index).
    - Certificate Owner Information.
    - Snapshot of physical certificate.
  - QR code.
- Verifies the certificate using:
  - Hash value extracted from a QR code.

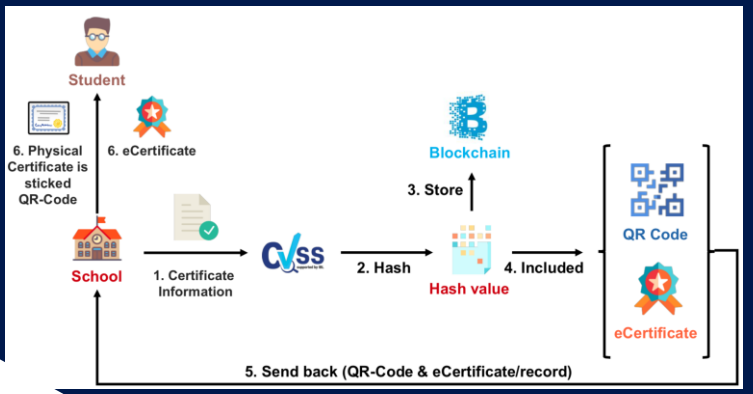


Figure 2: Issuing process

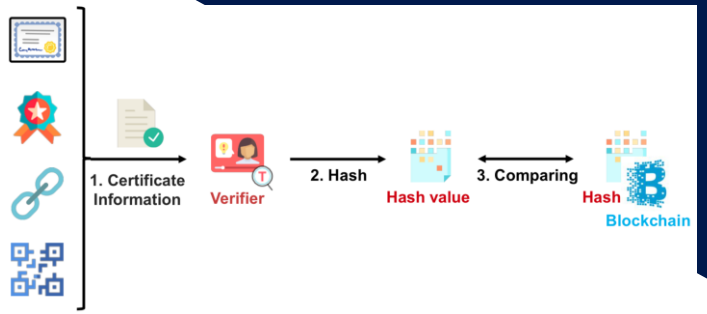


Figure 4: Verifying process

Add a fooNguyen, Duc-Hiep & Nguyen-Duc, Dinh-Nghia & Huynh-Tuong, Nguyen & Pham, Hoang-Anh. (2018). CVSS: A Blockchainized Certificate Verifying Support System.

Related Work (3/3)

Developing Ethereum Blockchain Based Document Verification Smart Contract for Moodle Learning Management system. (2018)

- Technologies used:
  - Ethereum Virtual Machine (EVM).
  - Solidity.
  - Smart Contracts .
- Outcome:
  - E-cert.
  - Document (Certificate) Authentication Code for verifying.

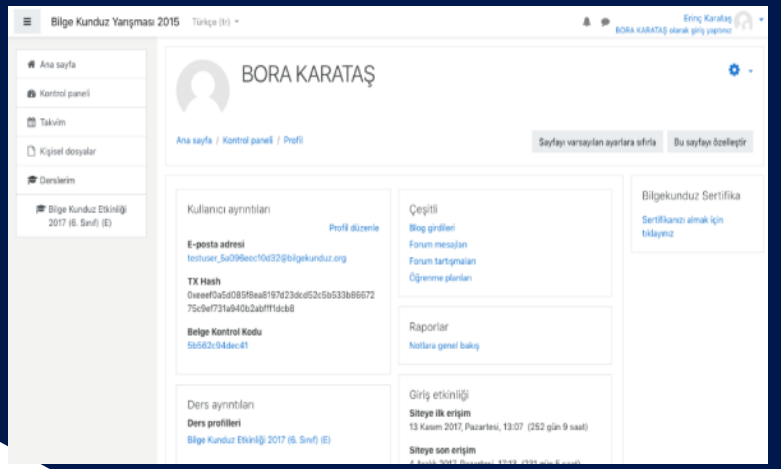


Figure 5: Student Profile Page.

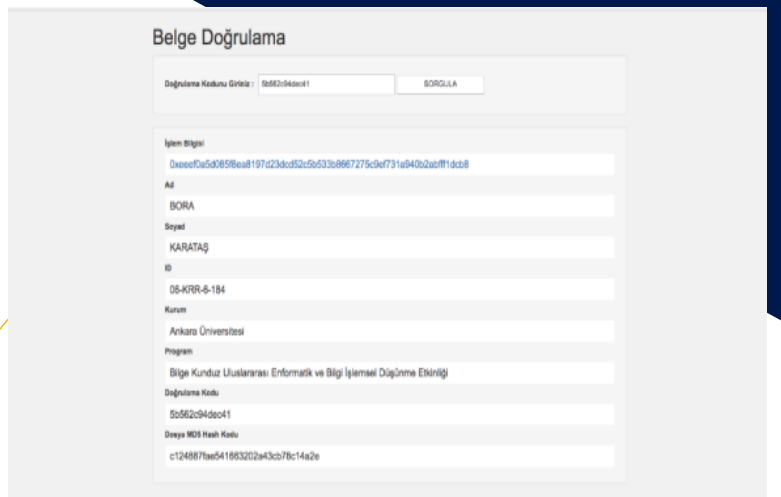


Figure 6: Document Verifying Page

KARATAŞ, E. (2018). Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System. International Journal of Informatics Technologies, 11 (4), 399-406. DOI: 10.17671/gazibtd.452686

Problem Statement

The problem here is the wide forgery of School, Bachelor and Masters Degrees in Egypt which may have disastrous impact on the society and the inconvenience of the process of requesting and issuing a certificate and the huge waste of time it costs.

Intro to Hyperledger Indy

- Public Key Infrastructure (PKI).
- Pool.
- Credential.
- Decentralized Identity (DID).
- Schema.
- NYM transaction.
- Roles.
- Proof of claim.
- Verification.

System Overview (1/3)

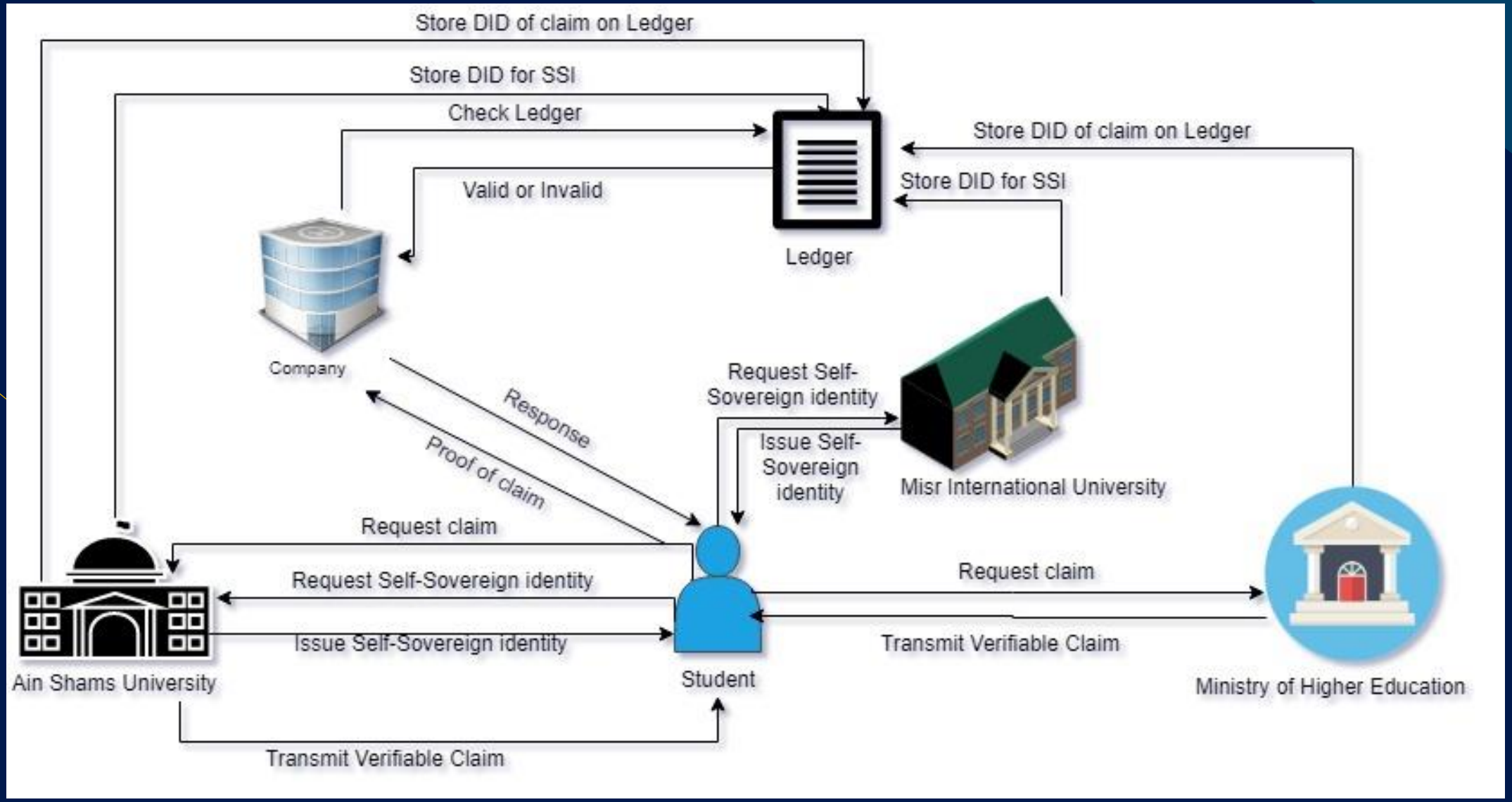


Figure 5: System Overview.

System Overview (2/3)

- Student requests Self Sovereign Identity from the university that he/she enrolled in it.
- University/ Ministry of Higher Education store DID of the SSI in the ledger
- Then, student request claim from the university.
- University/ Ministry of Higher Education transmits Verifiable claim and store DID on the ledger.

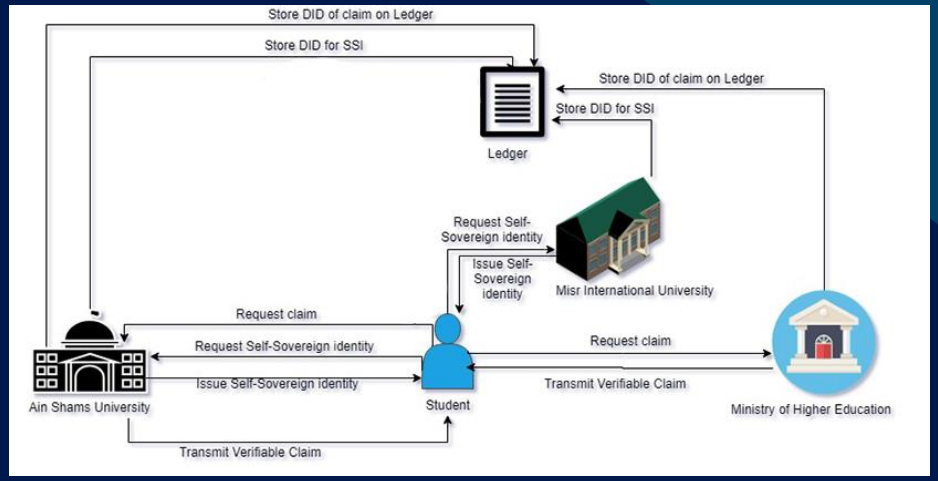


Figure 5: Student role.

System Overview (3/3)

- Company requests Proof of Claim from applying student.
- Then, the company checks for the validity on the ledger.
- It then respond to the student for the validity of it.

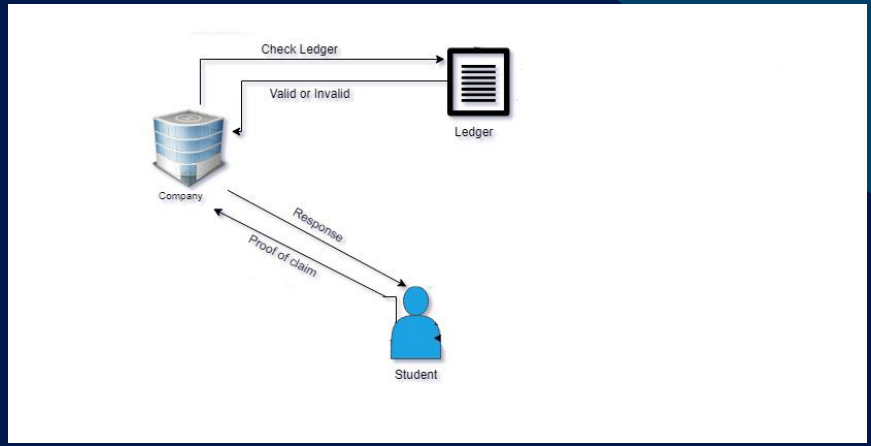


Figure 5: Company role.

Expected Result

- Ministry of Education and Ain Shams University will be able to put students certificates on the blockchain.
- Students will have easier access to their certificates than the traditional way.
- Companies and employers will be able to verify the certificates of their employees or who applied for a job.
- Securing the certificates from forging.

Demo

Any Questions?

Thank You