Software Proposal Document for project Digital Certificates Authentication Using Blockchain

Alley Mostafa, Sherif Abd El Khalek, Mohamed Reda, Shehab El-Din Mohamed

March 19, 2020

Abstract

The forgery of certificates is a widespread long term problem in the academic community of Egypt , it is pretty common to get a fake certificate that claims you have graduated from a university and apply for jobs easily. For that problem , the Blockchain technology which is known for its reliabilty and trust is used as a solution for this problem , our proposed system which aims to create a tracker for the certificates achieved by a student throughout his whole educational career and storing them in a disturbed de-centralized network in the form of digital certificates which can be easily verified , thus making the process of verifying the certificates easier and effortless. This will be implemented with the use of Linux's foundation hyperledger fabric or Indy which is still a choice to be made since both platforms have their owns pros and cons.

1 Introduction

1.1 Background

According to the Kuwaiti newspaper Al-Qabas 94% of the forged certificates were Egyptian and that 47 cases of fraud in scientific certificate were seized during 2018, it was pointed out that 44 of them were Egyptian universities[1]. A report which caused a lot of controversy and accusation until the Egyptian embassy in Kuwait stated that the forged certificates were forged by a fraud network. So, in order to solve this problem of forged certificates a digital certificates system based on blockchain was proposed. A system that takes advantage of the blockchain properties which are consensus, provenance, immutability and finality.There are alot of different blockchain platform but mainly this proposal will be focusing only on Ethereum and two of The Linux Foundation hosted projects Hyperledger Fabric and Hyperledger Indy.

1.1.1 Blockchain

The first introduction of secured chain of blocks using hashing was introduced in 1991 by Stuart Haber and W. Scott Stornetta [2] and its purpose was to make a

system for documents where their timestamps couldn't be tampered. While the first blockchain was invented and developed by a pseudonymous person called Satoshi Nakamoto with the purpose of developing the bitcoin. The blockchain is a list of blocks with each block mainly having data, the hash of the data and the hash of the previous block as in Figure 1. Those blocks are distributed across a shared ledger which everyone running the network holds. This make the blockchain tamper proof since firstly, a change in block data will lead to the change in its hash therefore the next block previous hash will need to be changed which will lead to the change of the of next block's hash and the same process continues till the last block. Secondly, since the blockchain is distributed across a shard ledger this means that those process of altering the blockchain needs to be done on 51% of the nodes holding the blockchain.

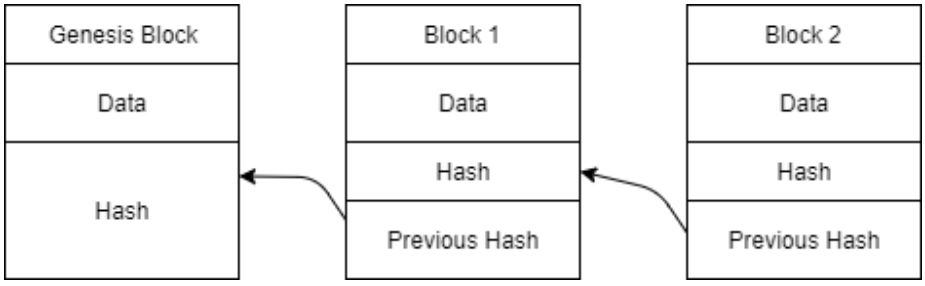

Figure 1: Blockchain

1.1.2 Consensus

Consensus Is the agreement between all participants on the network. A Set of rules that keep them synchronized and any transaction that doesn't follow this set of rules it's considered invalid.

1.1.3 Provenance

It means that any asset on the ledger can be tracked , where it came from and the change of its ownership back to its origin.

1.1.4 Immutability

Any of the participants on the network can't change the any transaction that has been recorded on the ledger as discussed previously while explaining the blockchain concept. In case of any inputting of wrong data while making the transaction a new transaction should be made to reverse this error but, still both will be available on the ledger with the first considered as an error.

1.1.5 Finality

It means that any transaction on the ledger is finalized , meaning that it can't be reverted which enhances the trust in the ledger.

1.1.6 The Linux Foundation

The Linux Foundation is an nonprofit technology consortium that hosts a lot of different open-source projects.Their main goal is to build sustainable ecosystems around open source projects to accelerate technology development and industry .Two of the projects they are hosting are Hyperledger Fabric and Hyperledger Indy.

1.1.7 Public Blockchain

Public blockchain is a decentralized ledger which means that every node on the chain has a copy of the ledger to insure immutability. In detail, this type of blockchain is append-only blockchain which means everyone on the chain can read and write transactions but nobody can edit or delete any records on the blockchain. Furthermore, this blockchain provides validating transactions by reaching a consensus and that means all nodes on the chain must verify the integrity of a transaction before it's put on the blockchain. There are some already made applications with uses the public blockchain such as the famous cryptocurrency BitCoin and the blockchain system Ethirum, both are open-source and anybody can join the network of them.

There are advantages of the public blockchain such as:

Security: the more nodes on the network, the more secure the blockchain as it provides more decentralization of the blockchain and also much more verifying nodes that can result in protection from attackers that want to take over the blockchain system.

Trust: This type of blockchain doesn't have any trust issues because of the number of nodes on the blockchain and that it's public so anyone can verify the transactions.

The disadvantages of public blockchain are:

Slow speed: Because of how big the network can get, this results in the massive decrease of the transactions processing time and also increases the time for the network to reaches consensus on it.

Resources: This network also can result in huge power consumption and this depends on how big the network is.

1.1.8 Private Blockchain

Private blockchain have a lot of similarities to the public blockchain. It can reach consensus with all the nodes in it. It can provide immutability to the transactions as no one can delete or edit transactions on it. It also provides provenance which means that it can track a transaction all the way back to its original source and that can benefit in the supply chain applications as it's a simple way to provide full detail about a product timeline. The private blockchain is a permissioned network that can only give access to some people only to write on it. As it's private network, this means it's a closed network so that not everyone can even access the transactions to read them, everything and everyone on the private blockchain will need access to it. This makes this type of blockchain more centralized as its closed network with only few nodes that are given access to it, it's not entirely centralized due to the number of verified nodes, it does make it more centralized than a public network. The private blockchain is perfectly designed for business network applications as companies always want more privacy on their customer credentials.

Private blockchain advantages are:

Fast: Since the private blockchain only running on few nodes, then this means it will reach consensus and will make transactions faster than the public blockchain applications.

Resources: As discussed earlier, as there are few nodes on the network, that makes the processing faster and also reduces cost of more computations devices.

1.1.9 Permissioned Blockchain

The permissioned blockchain is that not every node on the chain has access to write transactions, only nodes which have permission to write on the chain. This type of blockchain can either public or private blockchain. It adds a security layer on top of the blockchain that monitors the actions done by the allowed identities. The permissioned network is an advantage. As it increases its security as not every node has access to write transactions into it. Although, every node has the right to read any transaction or the transactions they want to verify. Its usually used by companies who wants more security on their network. The major disadvantage of this type of network is the compromising of it's internal security. It depends on the trust between the members on the network, as the number of nodes on the system is small, then this can result in bad actors compromising the system security.

1.1.10 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
Mode of Peer Participation	Permissionless, Public	Permissioned, Private	Permissioned, Public or Private
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

1.2 Motivation

1.2.1 Market Motivation

The main motive here is the huge need of Egyptian educational system for such a system the can prevent certificates forgery which is a thing that can be widely seen lately in Egypt.

1.2.2 Academic Motivation

The application is heavily inspired by previous projects of the same domain which are all aiming to end the problem of fake certificates and forgery. MIT has developed blockcerts which was the pioneer of digital certification using blockchain [5] , Duc-Hiep Nguyen, Dinh-Nghia Nguyen-Duc, Nguyen Huynh-Tuong, Hoang-Anh Pham developed the CVSS application which contributed with different technology which was Ethereum Blockchain [8] , Erinç Kratas aimed for a new education method without the need of school/college [4] in his digital certificate tracking application.

1.3 Problem Definition

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

2 Project Description

Introduce digital certificates for students to let companies and institutes be able to check whether the certificate was valid or not and giving them an instant feedback to their job application.

2.1 Objective

The objective of this study is to develop a system using Hyperledger Fabric or Indy. Those two frameworks fall under the Hyperledger project which is an open source project hosted by The Linux Foundation. The two Hyperledger frameworks are Blockchain frameworks, it will be used for developing a digital certificate system with a network of participants including the ministry of higher education and scientific research, public universities and private universities with the asset here being the graduates' digital certificates stored on the ledger for preventing forgery in college certificates in Egypt and providing reliable information regarding the certificates.

2.2 Scope

Our project will contain in its scope:

1. Different users (Issuer, holder, verifier).
2. Issuers issue/revoke the digital certificates to holders.
3. Holder has many digital certificates or identities.
4. Verifier validates the holder's digital certificate.

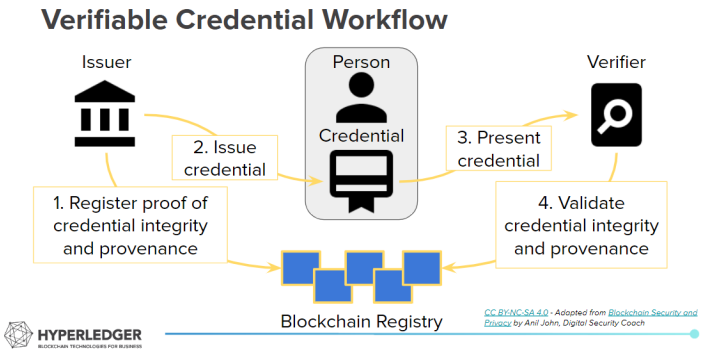

Figure 2: Verifiable Credential Workflow [14]

2.3 Project Overview

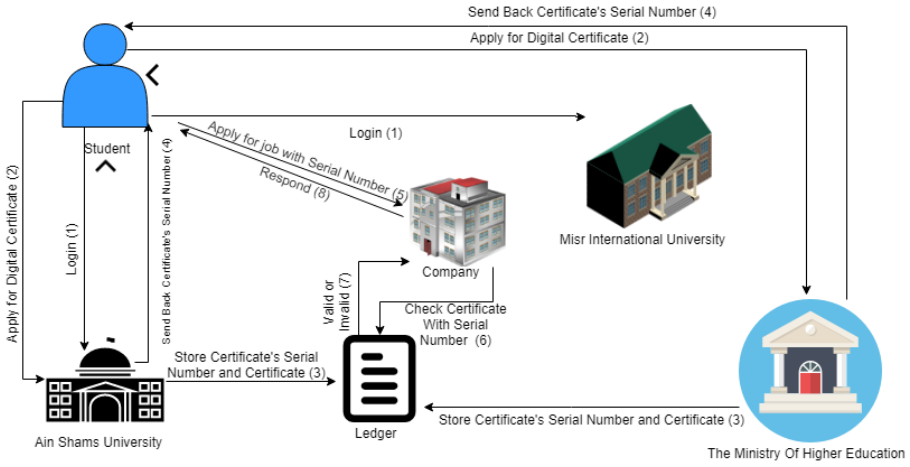

Figure 3: Workflow diagram

Student heard of digital certificate and when he went to the university, they asked him to make first Self-Sovereign identity. When he finished, student request the Ministry of Higher Education to send him verifiable claim to prove his certificate from his university to specific company. The Ministry of Higher Education creates digital identifier (DID) on the ledger associated with claim schema and with public key and creates document validity of the certificate signed with private key. Now the signed key in the ledger with DID of The Ministry of Higher Education. The company verifies the signed document using public key and make sure that the signed private key from The Ministry of Higher Education then take decision whether he was accepted or not.

3 Similar System Information

The benefits of the blockchain technology has proven to be very efficient and saves cost and time, therefore a lot of other governments and universities have been using blockchain to make an application for digital certificates using different methods to solve the problem of forgery.

3.1 Similar System Description

3.1.1 Blockcerts

MIT's(Massachusetts Institute of Technology) famous application blockcerts is one of the first blockchain solutisons made for the digital certificates , it's initially with the bitcoin blockchain application due to its trusted performance

but Ethereum support was added for the sake of testing for errors, Blockcerts may be considered to be one of the best mobile applications ever made in this domain yet it's doesn't lack its own problems, Although it includes all of the blockchain's benefits it has the issue of being extreamly critical when the user tends to use it , meaning one mistake made with the application will force the user the need to revocate which requires the permission of the the owner and the issuer, this of course doesn't work with different countries according to its regulations[5]

3.1.2 University of Jordan

Tarek Kanan , Ahamd Turki Obaidat , Majduleen Al-Lahham of the University of Jordan are the developers of Smartcerts who were inspired by Blockcerts which is the leading first digital certificate application , they used Ethereum Blockchain to take advantage of its Smart Contract which enables the system to follow certain busniess logic to run the process of the certificate verification , they also used Solidity and its IDE remix as a compiler in case of errors. They also needed to follow the steps of how a certificate is issued from the university to a ministry to a student through a series of interviews with students , professors and certain staff members. [11]

3.1.3 University of Taiwan

The University of Taiwan has developed a blockchain application for the aim of verifying digital certificates , The application was programmed on the Ethereum platform and was run by the EVM (Ethereum Virtual Machine) which is a blockchain app that the Developers issues to execute commands using Solidity programming Language. [3]

3.1.4 EduCTX

EduCTX is one of the newest blockchain solutions , it's made using the blockchain platform ARK since it's an open source platform and due to its flexibiltiy to work with different programming languages , EduCTX has a better presentation of the student's education as it tends to show all of the course details and achievements and grades throughout the student's carrer not just the certificate.[10]

3.1.5 University of Ankara

The University of Ankara in Turkey used Ganache to develop a smart contract on the Ethereum , Ganache is an Ethereual blockchain application was made to run at a certain localhost port. They also used Solidity language and used a certain IDE for it it's called Remix for the sake of writing an Ethereum-Based smart contract and it was important as it becomes important to have these enviroments for catching errors while the code is being written, The application's aim was also unique as it attempts to offer a new way of education where the student

doesn't need a school or college but can explore different learning enviroments. [4]

3.1.6 CVSS

HCMC University of Technology deployed the CVSS (Certificate Verification Support System) application using Ethereum Blockchain due to its dependency on smart contracts to link between different different entities of the contract which is useful since smart contract makes the busniess logic perfectly clear but some problems of Ethereum cannot be ignored since it has problems of its own such as scalability and operational cost , so it was important to think of deplyoing the application using other blockchain applications to optimize the benefits [8]

3.1.7 Government of Singapore

The government of Singapore and its national company Skillsfuture with Opencerts has successfully deployed a blockchain application that tracks the whole certificates achieved throughout a student's whole education and from this point all students will receive their graduation certificates on a blockchain system. [6]

3.1.8 University of Basel

The University of Basel has contributed greatly in association with Proxeus has developed a blockchain application for academic certificates , every student in a school/university can now register his/her own certificates , each certificate has its own special ID, this blockchain solution tends to have two major benefits : the first is the elimination of forgery of certificates , the second being facilitating the process of validating the certificate (using Proxeus technology) so now issuing certificates take less the cost and effort. [7]

3.1.9 University of St. Gallen

The University of St. Gallen in Basel was inspired by the blockchain application that was deployed in the year of 2018 by the University of Basel , and so they collaborated with blockchain startup company BlockFactory , together they created digital certificate authentication using Ethereum blockchain. [12]

3.1.10 University of Birmingham

The University of Brimingham has done a project to help in the verification of ceritificates. Their solution was inspired by the Massachusetts Institute of Technology Media Lab (MIT) project called BlockCerts. They explain how they managed to implement their solution to help students and employers to verify the certificates in a more fast way than the traditional way. [9]

3.1.11 Crypto Valley Conference

2018 Crypto Valley Conference on Blockchain Technology issued a paper in which it discussed how they integrated Internet of Things with Ethereum smart contract blockchain to help in facilitating the supply chain process. The paper explains that they chose Ethereum blockchain because of their light weight client the doesn't take a lot of storage. [13]

3.2 Comparison with Proposed Project

Point of Comparison	Framework Used	Network Type	Permission	Assets	Participants
Blockcerts	BitCoin Blockchain	Public	Not Permissioned	All types of Certificates	Institutes , Universites , School , Students
CVSS	Ethereum Blockchain	Public	Permissioned	Educational Certificates	Institutes , Universites , Schools , Students
EduCTX	ARK Blockchain	Public	Permissioned	Educational Certificates	Institutes , Universites , Schools , Students
Our System	Hyperledger Fabric/Indy	Private	Permissioned	University Certificates	Institutes , Universites , Schools , Students

4 Project Management and Deliverables

4.1 Tasks and Time Plan

Task	Start Date	End Date
Idea Discussion	18-7-2019	21-7-2019
Idea Research	21-7-2019	1-9-2019
Survey and Proposal	12-9-2019	8-9-2019
Implementing Prototype	4-10-2019	8-10-2019
Proposal Presentation	8-10-2019	8-10-2019
Designing Application	8-10-2019	30-10-2019
Implementing GUI Design	30-10-2019	12-11-2019
Designing Database	12-11-2019	20-11-2019
Designing Class Diagram	20-11-2019	27-11-2019
SRS Writing	27-11-2019	8-12-2019
SRS Presentation	8-12-2019	14-12-2019
Implementing Application	14-12-2019	5-2-2020
SDD Writing	5-2-2020	14-2-2020
SDD Presentation	14-2-2020	21-2-2020
Validation and Testing	21-2-2020	10-3-2020
Writing Paper	10-3-2020	25-3-2020
Delivering Papers	25-3-2020	1-4-2020
Writing Thesis	1-4-2020	20-5-2020
Delivering Thesis	20-5-2020	30-5-2020
Final Presentation	24-6-2020	24-6-2020

4.2 Budget and Resource Costs

- Cloud Service(AWS, IBM Cloud).
- Kubernetes cluster (K8S) (containing Hyperledger Fabric or Indy containers).
- Domain name.

References

[1] "Kuwait - Around 47 cases of forged science degrees discovered so far." MENAFN, Arab Times, 9,December,2018, https://www.menafn.com/1097808046/Kuwait—Around-47-cases-of-forged-science-degrees-discovered-so-far

[2] Haber, S. Stornetta, W.S. J. Cryptology (1991) 3: 99. https://doi.org/10.1007/BF00196791

[3] J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051. doi: 10.1109/ICASI.2018.8394455

[4] 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

[5] Oliver, Miquel; Moreno, Joan; Prieto, Gerson; Benítez, David (2018) : Using blockchain as a tool for tracking and verification of official degrees: business model, 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a digital future: Turning technology into markets?", Trento, Italy, 1st - 4th August 2018, International Telecommunications Society (ITS), Trento

[6] Mohit Sagar (6, may , 2019) Singapore Government uses blockchain technology to produce digital certificates for graduates) https://www.opengovasia.com/singapore-government-uses-blockchain-technology-to-produce-digital-certificates-for-graduates/

[7] Proxeus (19, September , 2018) Swiss University certificates turn tamper-proof thanks to blockchain https://medium.com/proxeus/swiss-university-certificates-turn-tamper-proof-thanks-to-blockchain-1d1eedaf7531

[8] Nguyen, Duc-Hiep Nguyen-Duc, Dinh-Nghia Huynh-Tuong, Nguyen Pham, Hoang-Anh. (2018). CVSS: A Blockchainized Certificate Verifying Support System. 10.1145/3287921.3287968.

[9] Rujia Li, Yifan Wu, IT Innovation Interns (2018) Blockchain based Academic Certificate Authentication System Overview https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf

[10] Sayed, Rakibul Hasan Potential of blockchain technology to solve fake diploma problem Jyväskylä: University of Jyväskylä, 2019, 71p. Information Systems, Master's Thesis https://jyx.jyu.fi/bitstream/handle/123456789/64817/URN

[11] Kanan, T., Obaidat, A. T., Al-Lahham, M. (2019). SmartCert BlockChain Imperative for Educational Certificates. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). doi:10.1109/jeeit.2019.8717505

[12] Fintechnews Switzerland (21,September , 2019) Swiss University rolls out blockchain project to fight fake diplomas https://fintechnews.ch/blockchain$_b$$itcoin/swiss - university - rolls - out - blockchain - pilot - project - to - fight - fake - diplomas$/30788/

[13] Hinckeldeyn, J., Jochen, K. (2018). (Short Paper) Developing a Smart Storage Container for a Blockchain-Based Supply Chain Application. 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). doi:10.1109/cvcbt.2018.00017

[14] Kyle Den Hartog, Evernym. Hyperledger Indy Ambassador (2018) Hyperledger Indy Agents https://kyledenhartog.com/assets/Resume-KyleDenHartog.pdf