

CryptoCert — A Blockchain based Academic Credential System

Abstract

The benefits of blockchain can be used to improve traditional systems in just about any domain. Lots of research is still ongoing on how to utilize blockchain in industries such as healthcare, education, and finance, just to name a few. This paper proposes to use these benefits in the field of academic credential verification. Replacing current verification systems in educational institutes with those based on blockchain proves to benefit all the stakeholders. The paper evaluates this proposal and presents a prototype, CryptoCert, as a proof of concept. By removing the need for a third-party for verification, a lot of time and money will be saved for the stakeholders. More importantly, blockchain's immutability provides a unique and efficient way to curb the widespread fraud and falsification of academic credentials such as degrees, transcripts, and learning achievement certificates.

Keywords blockchain, academic credentials, certificates, education

1 Introduction

Blockchain was first implemented as the core idea behind Satoshi Nakamoto's whitepaper introducing Bitcoin [10]. Although the original intention of the paper was to introduce decentralized cryptocurrencies, the benefits of blockchain can be applied to a variety of fields today, including education [9], healthcare [21, 30], and land records management [24]. It is even being used to disrupt traditional computer science domains such as cloud [22] and privacy-preserving [23].

The main benefits that implementing a blockchain bring to the table are disintermediation (removing the need of third parties), decentralization, security (immutability), permanence, and computational trust. All the industries mentioned above can benefit immensely by harnessing these advantages. In particular, by implementing disintermediation, a huge amount of time and money in the form of administrative overheads can be saved, and used instead for more important actions.

Academic credentials play a very important role in a student's career. They stand as a proof of achievement for all the work the student has done. These include degrees, transcripts, and learning achievement certificates. However, presently there is a lot of fraud

and malpractices in this field. The issuance of fake degrees and certificates is especially prevalent in a developing country like India, which is where we reside.

A fake degree that can fool even the most rigorous inspection can be bought for as low as Rs. 2000 (around \$30) [1]. According to the University Grants Commission (UGC) of India, the capital New Delhi itself has 66 colleges issuing degrees without their permission [2]. India is also infamous for their ‘diploma mills’, which are basically fake universities that grant degrees for a fee, without providing any educational training [3].

Many efforts have been made to make this process more secure. In the case of physical certificates, efforts have been made to add watermarks, or barcodes to them to make them tamper proof and detect any attempt of alteration [4, 5, 6, 7]. However, the problems that exist with general paper certificates are still there, such as issuing multiple certificates for multiple verifiers, and being dependent on the issuer every time you want to issue a new certificate.

Significant strides have also been made in the case of digitizing certificates. However, most of the solutions depend on digital signatures. This means that the student is again dependent on the central public key infrastructure authority [8], and if something were to happen to it, their certificates would be lost forever.

Using blockchain instead of the above described systems will remove the risk of fraud and malpractices. Moreover, the student will never have to worry about the issuing institution closing down or being destroyed. The lifelong achievement record of the student will be permanently and securely stored in the blockchain [9]. The benefits of using blockchain for this purpose are explained in more detail in section 2.3.

This paper focuses on the possibilities of integrating blockchain technologies into the domain of education, more specifically in academic credential verification. It begins by presenting all the background and concepts of blockchain and how it benefits education. Then, it reviews the existing literature, after which it presents a prototype, CryptoCert, that tests and validates all the claims made throughout the paper. It summarizes all relevant information relating to the particular problem of academic credential verification, including the blockchain technologies we used. It ends with results and discussions, along with the scope for future work.

2 Background

2.1 Blockchain

A blockchain is essentially a distributed ledger, containing information in it. The main advantages of this ledger over traditional databases are its immutability and integrity. Once data is stored in a blockchain, it cannot be removed or changed. Its integrity is preserved by the fact that anyone can view the entire history of this ledger, unedited. Furthermore, this ledger is decentralized. This means that any stakeholder has their own copy of the ledger and can view and verify it at any point of time. This removes a single point of failure. The only way to completely destroy a blockchain, and in turn, lose all the data, would be to destroy each and every node that is participating in the blockchain protocol. In the current scenario, this would entail destroying millions of computers.

Another key feature of a blockchain is that it is very secure. The only known way to introduce fraudulent records or transactions into the blockchain is the 51% attack. This attack is only possible if 51% of all the nodes in the blockchain come under the control of a malicious organization. This is almost impossible, given the sheer amount of nodes in every popular blockchain these days.

Lastly, the most important feature of a blockchain is that it removes the need for a central authority of trust. Trust is instead maintained through computational power. Participants trust the nodes that have expended the most computational power. This is explained in detail in the next section.

2.2 Functionality of a Blockchain

Although the core technical details of how a blockchain works are quite complex, the gist of it can be explained in a lucid manner. A blockchain, in its simplest terms, can be thought of as a distributed ledger, with a copy of the ledger being in the possession of all the stakeholders, at all times. How can we ensure that each and every participant (hereby referred to as a node) would have the same copy of the ledger, and be confident that whatever transactions are stored in it can be trusted? This is achieved through what is known as a consensus protocol.

First, whenever a node wants to add a new record to the blockchain, they broadcast a digitally signed transaction to the network. Signing the transaction proves that the message is indeed coming from the sender, preventing repudiation. Next, special nodes known as miners

listen to multiple such transactions, and collect them into a block. After this, each of these miners immediately engage in solving a cryptographic puzzle that is based on the block. It is a sort of miniature lottery, which utilizes computing power to solve. This lottery is known as **Proof of Work (PoW)** [10].

Whoever wins this lottery is said to have mined the block, and is allowed to broadcast it to all the nodes. A block is only accepted by a node if it has been mined. This can be easily verified by a node, by checking the solution to the cryptographic puzzle. The block is then added to all the previously mined blocks, hence the name blockchain.

All the blocks are temporally linked to each other, by including the hash of the current block in the header of the next one. This ensures a block's immutability, as changing even a single character in any one of the blocks will change its hash, which won't match with the hash in the next block's header, thereby invalidating the blockchain.

The miner who wins the lottery is rewarded for his efforts by receiving some cryptocurrency. This compensates for the electricity and computational time spent by him.

Putting all this together, in order to fool the blockchain, the malicious nodes will have to keep winning this lottery every time. As long as they don't have control of over 51% of the nodes in the network, doing so is probabilistically impossible. Therefore, as long more than 51% of the nodes are operated by honest people, it is impossible to introduce a new record into the blockchain without consensus. Even if a malicious node is able to mine a fraudulent block once or twice, the nodes always accept the longest chain. Thus, eventually the honest nodes will overpower the malicious ones.

This is how a blockchain removes the need for a central authority to verify each and every transaction. Trust is instead shifted to computational power and cryptography. In other words, implementing a blockchain leads to a **trustless** system.

2.3 Blockchain in Education

The above described qualities of the blockchain can be effectively harnessed to improve on the current education system, especially in the domain of verifying and issuing academic credentials. Presently, there is widespread fraud in this area. Blockchain can solve this problem by providing a decentralized way for stakeholders to verify a document holder's credentials. Moreover, the verifier can trust that the credentials stored in the blockchain have not been tampered with (due to its immutability). Additionally, because of its permanence,

data once stored in the blockchain can never be removed or edited, thereby keeping all its transactions public and open.

Most importantly, blockchain removes the need for the verifier to contact the issuer in order to validate the credentials. The verifier can directly query the blockchain, and if the data in the blockchain is to their satisfaction, they can rest assured that the certificate is indeed valid, from the claimed issuer, and not been tampered with since it was uploaded to the chain. The 3 main stakeholders involved are:

1. **The Issuer:** This can be the university that wishes to issue certificates, diplomas, degrees or transcripts to the blockchain. It can also be massive online course organizations such as Coursera, Udemy, and edX, who wish to certify student achievements directly to the blockchain. It can also be extended to include organizations such as Open Badges (<https://openbadges.org/>), who wish to issue informal learning achievements of students to the blockchain.
2. **The Verifier:** This includes the employer, who wishes to verify an employee's academic credentials. It can also include banks, who wish to verify academic credentials for the purposes of extending loans. Moreover, it can also include higher education universities themselves, who wish to verify the credentials of a student applying for higher studies.
3. **The Student or Recipient:** These are the recipients of the academic credentials uploaded to the blockchain.

2.4 Problems with Traditional Systems

The current system of physical academic credentials is very susceptible to potential frauds and malpractices. It also leads to a lot of administrative overheads, wasting a huge amount of time and money.

More importantly, physical certificates are almost completely dependent on the issuer. If the issuing authority somehow closes down, goes bankrupt, or is unfortunately destroyed in a natural disaster, proof of the student's achievement is lost forever.

Some of the major obstacles faced by using physical certificates are:

- Every time the student has to send his transcripts to a verifier, he has to contact the university's concerned department, pay them money, wait a few days, and then go and collect it.

- Sending the credential to the verifier is completely dependent on the courier service.
- For the issuer, lot of time, money, and materials such as paper are wasted printing and authorizing the same credential.
- For an employer, to verify the credential, he has to contact the concerned issuer for each and every academic credential sent by the potential employee. He has to then repeat this process for thousands of potential employees, wasting a ton of time and labour.
- If the student is a refugee, and is fleeing to another country, he has no way to prove his existing academic credentials.

2.5 Problems with Existing Digital Certificates

Digital certificates eliminate a lot of the problems listed above, mainly those of storage and transportation. However, many problems still remain:

1. A digital certificate's integrity relies on digital signatures. These signatures, although definitely an upgrade on physically printed credentials, still need to be stored and issued by a central key repository. This means trusting a central authority, which in turn leads to another single point of failure.
2. If somehow the key infrastructure is destroyed or lost, the certificates become unverifiable forever.
3. The employer will still have to contact the issuing authority for their public key, in order to confirm their identity. This leads to even more time wasted.

Overall, we can clearly see how much time, money, labour, and material is unnecessarily wasted in the current system of academic credential verification. As we'll discuss in the next few sections, implementing a blockchain based system will eliminate the need for a lot of overheads, and will allow for these resources to be allocated to much more important and urgent tasks instead.

3 Related Work

There have been many attempts at building blockchain-based systems that issue degrees, documents, and learning certificates to the blockchain. Most of these attempts have some limitations, which we will explain in section 6. There are mainly two types of implementations, some which are software implementations, and others which are research based discussions. We will discuss them both in this section.

Sony Global Education [11, 12] has decided to use Hyperledger Fabric to create a custom blockchain and to host that system using IBM's cloud, which will provide the network infrastructure for issuing and verifying educational records. It will also track a student's learning progress throughout his education. It will provide a transparent and validated record of all the student's achievements. SAP [13] is developing a set of command-line libraries that use the Ethereum public blockchain to issue records of academic achievement, which they are piloting for a specific class on the OpenSAP MOOC.

Learning Machine and MIT [14] launched a system for issuing blockchain-based verifiable records to students (<https://www.blockcerts.org/>). It is the only fully developed and open source implementation currently available. First, the issuer invites the student to receive a blockchain credential. Once the student accepts the request, the issuer send him his blockchain and address, and then proceeds to store a hash of the document on the blockchain. He then finally sends the credential back to the student. When a verifier wants to verify the student's credential, the student sends them their blockchain credential. The verifier in turn looks up the same credential on the blockchain. If both the credentials match, the verifier accepts the document. Educhain (<https://educhain.io/>) is a company based in Dubai [15] that enables instant issuance and authentication of digital records for institutions, corporates, and governments using blockchain. It provides a digital wallet, in which all of the student's achievements can be stored, and later verified by any potential employer or university.

Calicut University plans to use blockchain technology [16] for digital certification and validation of academic certificates and mark lists. University of Nicosia was the first university to issue a student's credential to the Bitcoin blockchain for their own MOOC [17].

Now we will review the research literature published related to the topic. Sharples and Domingue [18] analyzed the use of blockchain in academics. First, they discuss how the blockchain can be used to develop a system of consolidated academic records for a student,

such as their transcripts, certificates, and achievements. Then, they proposed a distributed system for recording intellectual effort and ideas. They also proposed an intellectual currency called KUDOS, which could be used to establish a reputation based system for all academic institutions. It can then be used as the sort of cryptocurrency for the blockchain, and traded between the institutions and students to issue or verify certificates.

Gräther et al. [9] proposed and evaluated a blockchain based system for issuing and verifying certificates. They listed the benefits for the three main stakeholders: students, employers, and institutions. Finally, they described in detail a conceptual architecture which could implement the discussed features. They also discussed a prototype of the implementation they built and how it performed on an evaluation with the stakeholders.

Gresch et al. [19] discussed the implementation of a blockchain based system in the University of Zurich (UZH) for the issuance and verification of diplomas. Their aim was not to build a universal system, but a system to specifically help UZH to issue student diplomas to the Ethereum Blockchain. They discussed the requirements of the records issuance and IT offices of the university. They then proceeded to build a prototype on the Ethereum blockchain using smart contracts. Finally, they discussed how their specific prototype satisfies all their desired requirements.

They implemented a basic system, in which first the hash of the diploma's PDF is uploaded to the blockchain. It included a front end which communicated directly with the Ethereum blockchain. Whenever a verifier wished to verify a diploma, they used the front end to get the hash of the student's document, and compare it with the hash stored on the blockchain, thereby validating the diploma without ever contacting UZH.

Palma et al. [20] implemented a prototype for storing Brazilian higher education degrees to the Ethereum blockchain. They worked alongside the government and relevant authorities to implement an integrated degree issuing system for higher educational institutes in Brazil. They used the Brazilian Public Key Infrastructure for the purpose of digital signing. Their implementation made use of several smart contracts which ensured that only valid institutes can issue these degrees.

Further, they proposed a unique concept using smart contracts. They suggested that smart contracts could be used to keep track of a student's entire credit and course history. Then, when all the requirements were objectively complete, the contract could automatically

issue a new degree for the student to the blockchain. This completely automated process can save a lot of time and money for the issuers, verifiers, as well as the students.

Blockchain in Education by Grech et al. [8] is a comprehensive overview on the use of blockchain technologies to improve on current educational systems. It was published by the Joint Research Centre (JRC), the European Commission's Science and Knowledge centre. Its main aim was make the European policy makers aware about this new and potentially disruptive domain. After discussing in great detail about all the facets of this technology, they finally concluded with a set of advises to the European policy makers, which would help them in implementing, monitoring, and making laws for this domain. Following are the main conclusions:

- Blockchain technology will accelerate the end of a paper-based system for certificates.
- Blockchain technology allows for users to be able to automatically verify the validity of certificates directly against the blockchain, without the need to contact the organisation that originally issued them.
- The ability of blockchain technologies to create data management structures where users have increased ownership and control over their own data could significantly reduce educational organizations' data management costs.
- Blockchain-based cryptocurrencies are likely to be used to facilitate payments within some institutions.

We will compare all these existing implementations with each other, as well as with the one we propose in section 6.

4 The Proposed System

Almost all the implementations and literature evaluated in section 3 proposed to only store the document hash in the blockchain. Then, the student had to send the document to the verifier, who hashed it again to compare it against the hash stored in the blockchain. Only [20] proposed something different, by suggesting to store all the student's credits as well as course history in the blockchain, in order to automatically issue diplomas later. What we propose is more unique, robust, and secure. We propose to upload the entire credential, i.e. the entire degree, transcript, or learning certificate, to the blockchain. This is better than the existing systems in two areas, namely efficiency and robustness. In the case of efficiency, it removes the need to compute the document hash at two separate ends. In the case of robustness, it is much more secure and permanent to store the entire credential to the blockchain. The hash of a document is very sensitive and even a small inadvertent change could lead to a big misunderstanding between the stakeholders. On the other hand, storing the entire credential is much more secure, robust, and fault tolerant. A minute mistake in uploading the certificate won't impact the core details of the credential a lot. Moreover, seeing the entire credential being stored in the blockchain will give the verifier much more confidence that the document is original and has not been tampered with.

Another difference in our implementation is the use of a Central Issuing Authority that will grant the institutes the power to issue credentials. This will help the government to continue monitoring the issuance of major credentials such as diplomas, and will also prevent fake, malicious, or unknown institutes from issuing credentials to the students.

4.1 Choice of Blockchain

There are mainly three different types of blockchain architectures, namely public, private, and consortium [21]. For our proposal, the public blockchain architecture ticks all the boxes, because of the following reasons:

1. A private blockchain is controlled by some authority, who decides which node can make transactions, and who can verify them. This destroys the whole purpose of a free and open blockchain, which created the decentralized paradigm in the first place. It leaves a bit too much control in the hand of a few special nodes. Therefore, the verifier cannot completely trust the credential.

2. A large public blockchain provides a ready to use place to develop applications on top of it. It saves a lot of developer time which would have been used to develop a completely new and customized blockchain.
3. Lastly, a large popular blockchain already has a known factor of trust, as it is already being used for important transactions such as financial ones. Moreover, they already have millions of nodes in the network, which makes them even more secure, robust, trustworthy, and efficient to use.

4.2 Architecture and Design

Our proposed system is divided into three parts: the proposed architecture, the issuing of a new credential, and finally the verification process. But first, we present the overall workflow in Figure 1.

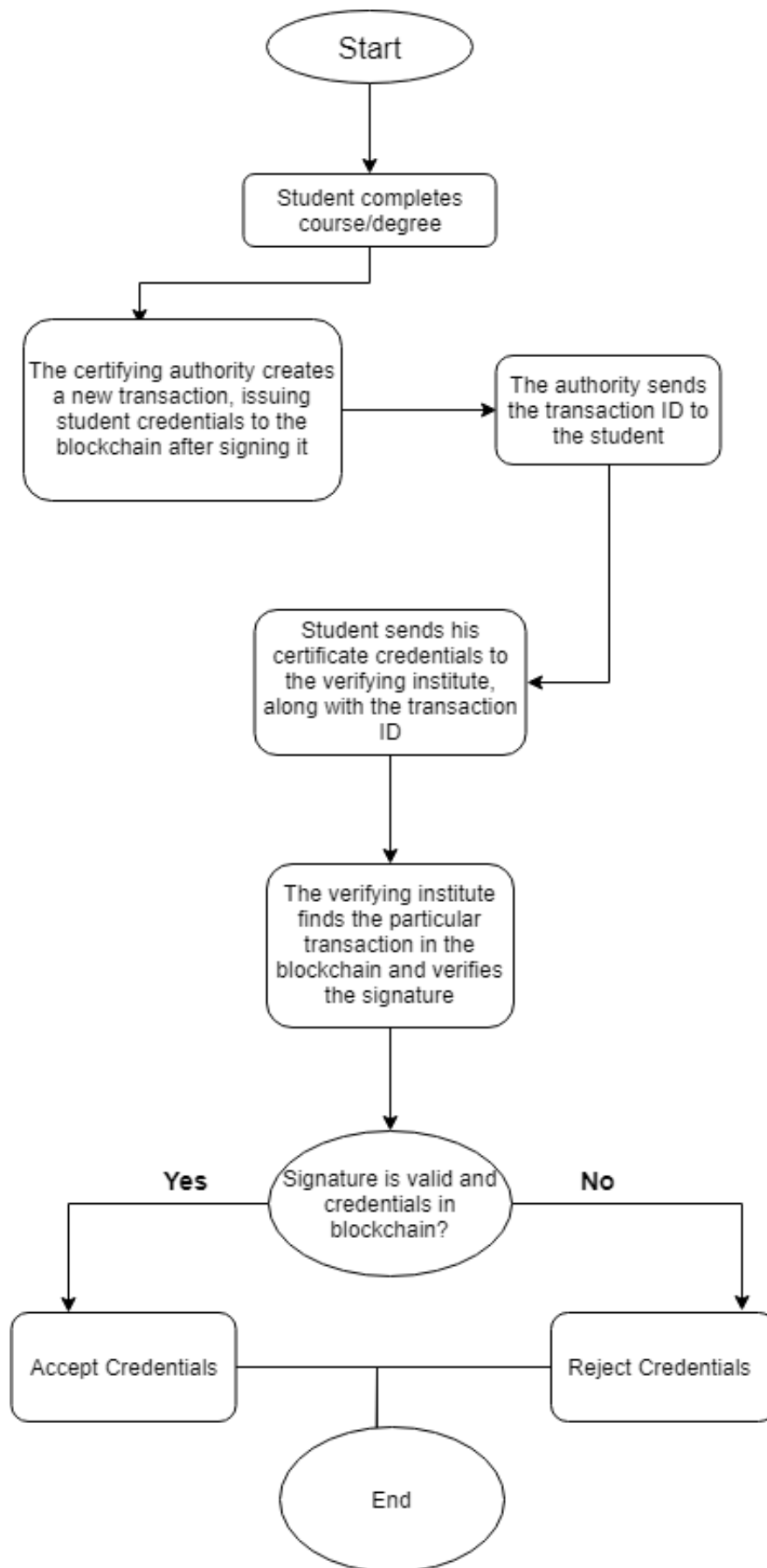


Figure 1 - The Overall Workflow

Next, the proposed central architecture of our proposal is given in Figure 2.

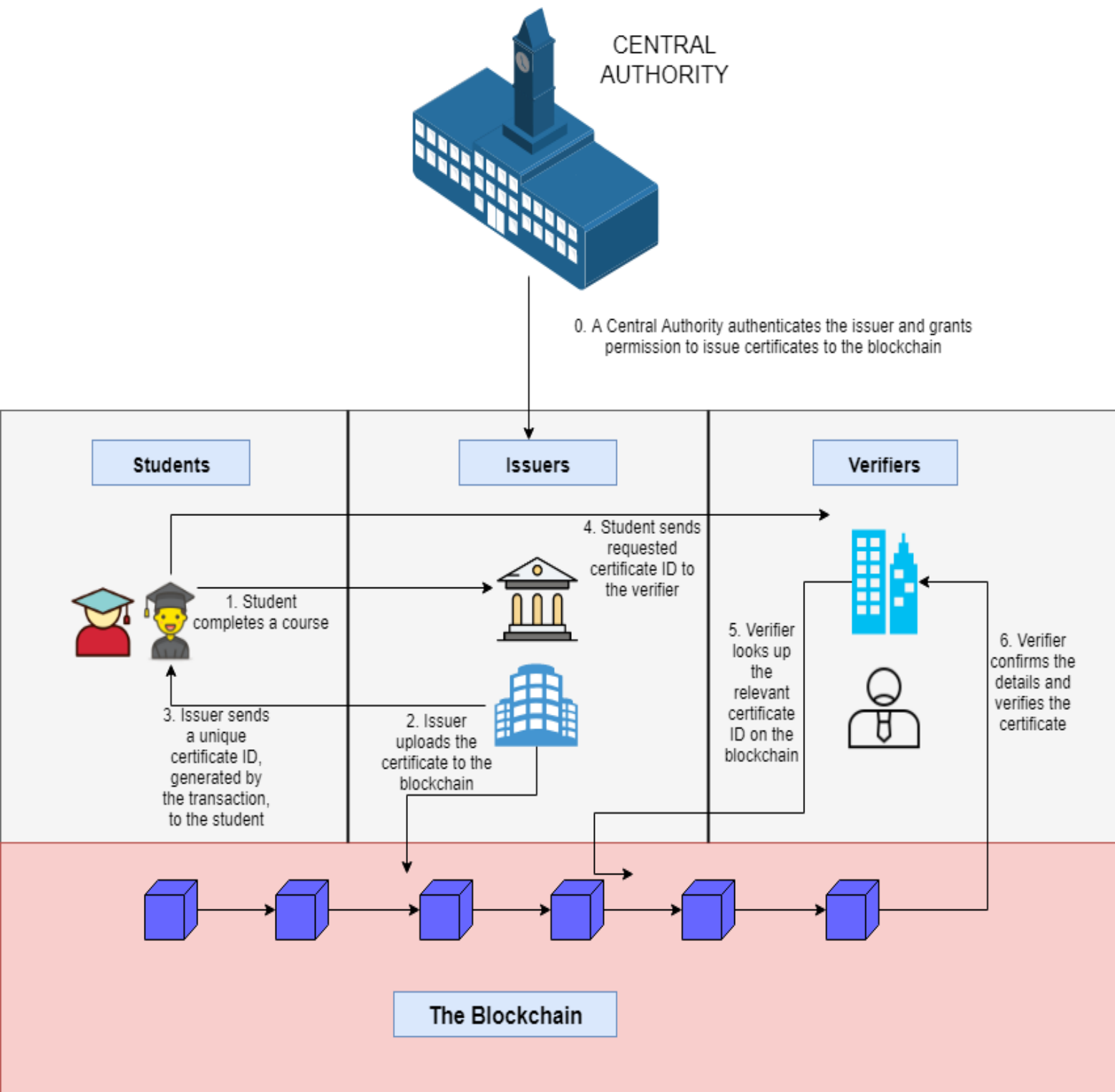


Figure 2 - The Proposed Architecture

Now, we present the design for the Issue Module. It will be used to upload the academic records (transcripts, certificates, skills etc.) to the blockchain after approval from the institution. We have designed an easy 6-step process as given in Figure 3.

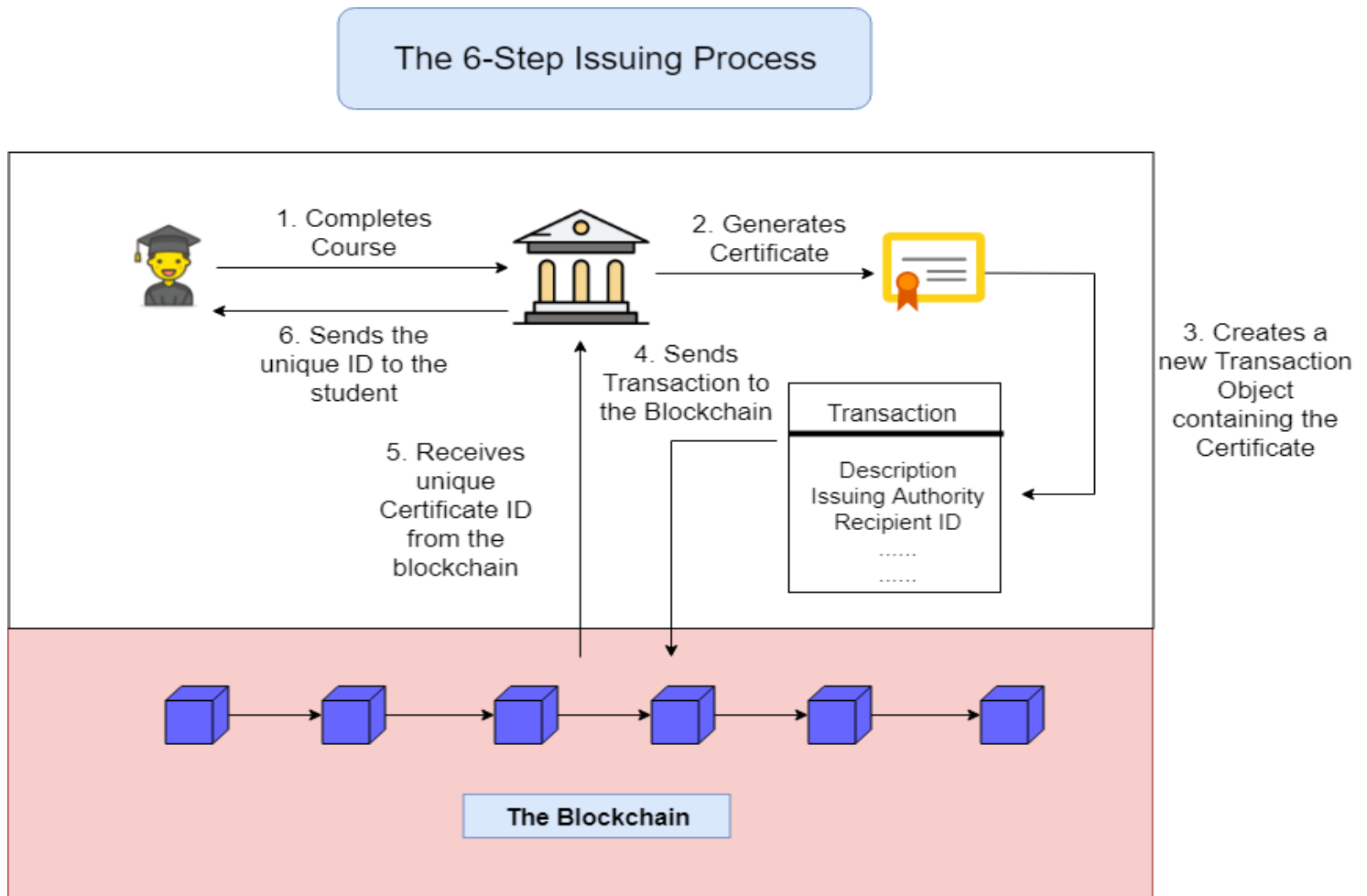


Figure 3 - The 6-Step Issuing Process

Now, we present the design for the Verification Module. It will be used by institutions such as universities, employers, and banks to verify a person's records on the blockchain, without the need to involve the original institution. It is designed as a 5-step process in Figure 4.

The 5-Step Verification Process

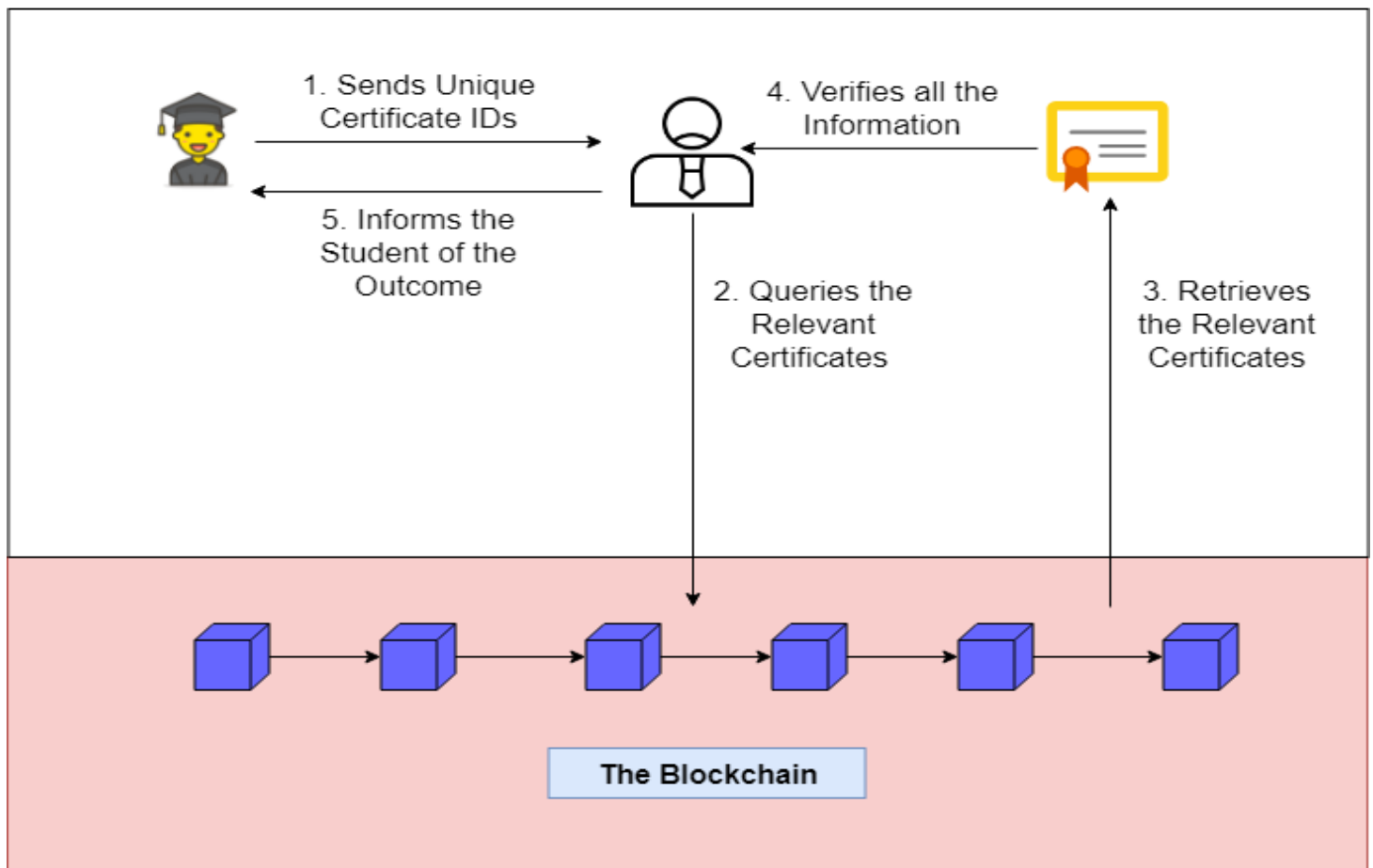


Figure 4 - The 5-Step Verification Process

The exact details, workings, and implementation of the above architectures are presented in section 5.

4.3 Contents of a Block

A single block in the blockchain of our proposed system will have a series of transactions, with each transaction storing a single credential.

As discussed in this section, our proposal is going to upload the entire credential instead of just its hash. Therefore, we need some sort of JSON schema which will fit our

certificate model. We have designed a unique certificate structure, which will be uploaded to the blockchain in the final implementation. It is given in Listing 1.

```
{
  "id": "94893140015205396912602365356454288597831631616407868931102
234519522628457978",
  "description": "Solidity Tutorial",
  "issuingAuthority": "VIT University",
  "recipientID": "15BIT0102",
  "issuingDate": "Friday, April 5th, 2019, 3:15:10 PM",
  "typeOfCertificate": "Course Completion",
  "details": "Good performance!"
}
```

Listing 1 - The Certificate JSON

Each transaction in a particular block will store a unique credential in the form of the above structure. All transactions are then hashed and stored to a block, which is ultimately mined to the blockchain. Given in Figure 5 is the format of a transaction in our proposed system.

[block:4151985 txIndex:17] from:0xf97...95859 to:0x79a...7ca98 value:0 wei		Debug	^
status	0x1 Transaction mined and execution succeed		
transaction hash	0x486b917bc343ca63be638663170cc0e880db64824742c68f8adbc26bcf160ba3		
from	0xf97c2cb6b748529ff1c51906e340d28f6cc95859		
to	0x79a15abc48f41ffebafe079e6f04f3a70cc7ca98 0x79a15abc48f41ffebafe079e6f04f3a70cc7ca98		
gas	751223 gas		
transaction cost	751223 gas		
hash	0x486b917bc343ca63be638663170cc0e880db64824742c68f8adbc26bcf160ba3		
input	0xcac...00000		
decoded input	-		
decoded output	-		
value	0 wei		

Figure 5 - A Transaction

5 Implementation

5.1 Implementation Details

To demonstrate the proof of concept for our proposal, an Ethereum DApp (a distributed app deployed to the Ethereum blockchain) was built and deployed. It was then compared to our initial proposal and requirements, providing satisfactory results. Although there is a lot of scope for improvement (as discussed in section 7.2), the main purpose of this app was not to build a complete product, but to demonstrate the viability of our proposal, and to provide a valid proof of concept.

The DApp was built using the Solidity programming language and deployed to the Ethereum blockchain. It made use of the core concept behind Ethereum: self-controlled accounts known as smart contracts. All these technologies are explained in detail in the next few sections.

5.1.1 Ethereum

Ethereum is an open source blockchain infrastructure, introduced by a young computer scientist by the name of Vitalik Buterin in late 2013 [25]. He found the original Bitcoin implementation of the blockchain to be quite limiting and constricting. He envisioned that the idea of a blockchain could be expanded. Virtually any field involving digital storage could benefit from the decentralized, immutable, and secure blockchain.

Buterin found that to build applications on top of Bitcoin's already existing financial blockchain is really complex and limiting. In particular, the only way to store data other than financial transactions in the Bitcoin blockchain was to add it to an opcode (particularly the opcode `OP_RETURN`) of a new blockchain transaction.

Even if one were to do that, they'd still be limited by the 80 byte max size of the opcode, which would mean that they could at most store only a document hash in it. Moreover, there have been talks of Bitcoin planning to scrap the `OP_RETURN` opcode altogether, as they believe it is adding unnecessary clutter to financial transactions [20].

To overcome these limitations, Buterin co-developed the Ethereum blockchain, an open source platform which enabled easy development of blockchain apps on top of it. It contained all the good bits of the original blockchain idea, and then added the ability to build

unique apps that harness the power of blockchain on top of the existing financial blockchain. It also introduced its own cryptocurrency, called ether, to help run the blockchain.

As Ethereum met all our criteria mentioned in section 4.1, it was the perfect choice for our proof of concept.

5.1.2 Smart Contracts

The most well-known feature of Ethereum are its smart contracts. In the simplest terms, smart contracts can be thought of as computer controlled nodes running on the Ethereum network. They have their own address and ether balance. The main difference between a smart contract and a normal account is that smart contracts are completely autonomous agents.

In technical terms, deploying a smart contract to the network is just like adding any other transaction to the chain, the only difference being that the smart contract creation transaction will not have a “to” address, because it is not sending money to anyone. Once deployed to the network, they have to follow exactly the instructions that were coded into them before being deployed. Since the particular instructions (code) are deployed to the blockchain along with the contract, they cannot be changed and are present on every node in the network. Due to these qualities, a smart contract can be used as an intermediary between, say two businesses who do not trust each other, and can be used to mediate transactions between them.

For example, business A wants to only send money to business B when it completes a certain amount of work. This logic can be coded into a smart contract and then deployed to the Ethereum blockchain. Once it has been done, no one can alter the conditions, and when the conditions are met, it is guaranteed that the smart contract will automatically run, and perform the required transactions. In the case of our system, we do not particularly use the autonomous feature of smart contracts. Instead, we use a complementary feature that allows us to store data in the form of *structs* directly to the Ethereum blockchain. Once the data is stored in the blockchain using the smart contract, we can write code into it that will later help us retrieve that data at any given point of time.

5.1.3 Solidity Programming Language

Solidity is the language written by the Ethereum blockchain developers that is used to code smart contracts. It is a Turing-complete language based on JavaScript. It is a strongly-typed language.

Smart contracts are executed on the blockchain using the **Ethereum Virtual Machine** (EVM) that is running in the Ethereum Blockchain. The main function of the EVM is to convert the high-level solidity code into machine readable byte opcodes.

These opcodes are the core assembly level language instructions that actually run and carry out the contract instructions stored on the blockchain.

5.1.4 Building the Front End

The front end of our prototype, CryptoCert, was built using the React JavaScript framework. This choice was made looking at two main reasons. Firstly, the entire business logic while making a DApp is run on the front end. There is no server to which we can connect to retrieve information from the blockchain. We have to, instead, make use of the node running a full-copy of the blockchain on the client's side to retrieve information from it. Developing this logic using just plain, vanilla JavaScript would lead to really complex and long code. To avoid this, we decided to use React, which provides a fully developed JavaScript front-end library, that handles much of the dirty work for us.

Secondly, using React enables us to run our web server using NodeJS. This makes it much easier in the long run to host our website onto the real world, and also to use the plethora of amazing node packages available through the Node Package Manager (NPM), which make developing much easier.

Lastly, we have also used a sub-library of React, called Next.js, to seamlessly create a multi-page dynamic front end for our DApp. Next.js also provides server side optimizations which help the web page to load quicker.

5.1.5 Connecting the Blockchain to our Front End

In order to connect to the Ethereum blockchain to store and retrieve data via our front end, we used the **Web3.js** library. It is the missing piece that allows JavaScript in the browser (front end) to understand the solidity code stored in the blockchain, and execute commands

on it by directly connecting to the blockchain through the client's node. Figure 6 explains this process.

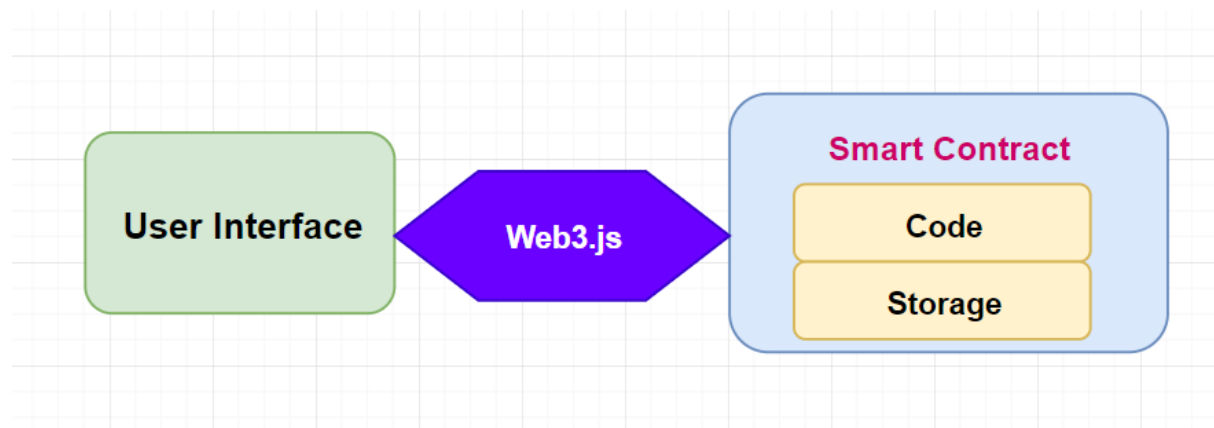


Figure 6 - The need for Web3.js

When the solidity compiler complies our smart contract, it throws out two main pieces of information (Figure 7) for each compiled contract: the bytecode, which is sent to the transaction which initializes the smart contract in the blockchain; and the ABI (Application Binary Interface), which is a JSON file that tells JavaScript exactly how to communicate with the blockchain through the smart contract. The ABI is what is given as an input to Web3, and tells it how to interact with the blockchain.

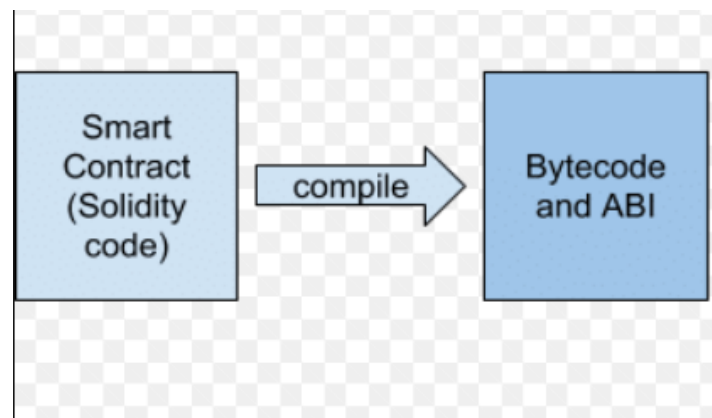


Figure 7 - The Solidity Compiler Overview

5.2 CryptoCert – The Prototype

This section discusses and showcase our prototype, CryptoCert.

5.2.1 The Smart Contracts

As explained in section 5.1, smart contracts are the core elements behind our implementation, and are the ones that communicate with the Ethereum blockchain to store and retrieve academic credentials. We are only going to discuss these smart contracts, as the rest of the code is out of the scope of this paper.

Our implementation made use of two smart contracts. The first one initializes the Central Issuing Authority. The Central Issuing Authority is the only entity (Ethereum account) that can add new credential issuers. This was done to prevent any random institute to impersonate another institute and start issuing certificates. It also ensures that only well-known and established institutes would have the power to issue academic credentials to students. This authority could, for example, be the education department of the government, which already has records of all the bonafide institutes, and can also be flexible enough to accommodate recognized online course organizations such as Coursera and Udacity. Note that this contract is only run once, in the beginning of the implementation. It is given in Listing 2.

```
contract IssuerFactory {
    address[] public issuers;
    address public centralAuthority;

    modifier authorized() {
        require(msg.sender == centralAuthority);
        _;
    }

    function IssuerFactory() public {
        centralAuthority = msg.sender;
    }

    function createNewIssuer(string name, address creator) public
    authorized {
        address newIssuer = new Issuer(creator, name);
        issuers.push(newIssuer);
    }

    function getIssuers() public view returns (address[]) {
        return issuers;
    }
}
```

Listing 2 - The Central Authority Contract

The second smart contract is the brains of our implementation. It is the one which initializes the issuer, and gives it the power to add new credentials, as well as retrieve previous ones. It also has some helper functions. Note that this contract ensures that only the issuer's address (Ethereum account) can be used to add new credentials, in order to prevent misuse. It is given in Listing 3.

```
contract Issuer {
    struct Certificate {
        uint id;
        string description;
        string issuingAuthority;
        string recipientID;
        uint issuingDate;
        string typeOfCertificate;
        string details;
    }

    address public issuer;
    string public issuerName;
    Certificate[] public certificates;

    modifier restricted() {
        require(msg.sender == issuer);
        _;
    }

    function Issuer(address creator, string name) public {
        issuer = creator;
        issuerName = name;
    }

    function generateID(string recipientID, string issuingAuthority)
private view returns (uint) {
        return uint(keccak256(recipientID, issuingAuthority, now));
    }

    function issueCertificate(string description, string issuingAuthority,
string recipientID,
        string typeOfCertificate, string details) public restricted {
        Certificate memory newCertificate = Certificate({
            id: generateID(recipientID, issuingAuthority),
            description: description,
            issuingAuthority: issuingAuthority,
            recipientID: recipientID,
            issuingDate: now,
            typeOfCertificate: typeOfCertificate,
            details: details
        });

        certificates.push(newCertificate);
    }

    function getNumberOfCertificates() public view returns (uint) {
        return certificates.length;
    }
}
```

Listing 3 - The Issuer Contract

Another unique thing we've implemented in the second contract is the use of the *keccak256* function. It is basically the same as the SHA3 hashing function [26], implemented for use in the Ethereum world. We have used this function to generate a unique certificate ID for each certificate. This ID is generated by hashing the certificate description, name of the issuing authority, and the current time. It is given to the student, who keeps it with him. Whenever the student wants to get a certificate verified, they send that unique ID to the verifier, who then compares it with the ID stored in the blockchain. As the ID in the blockchain is secure and immutable, if both the IDs match, then the certificate is valid. The verifier can then move on to check all the other displayed details of the certificate.

Notice how the employer did not need to contact the university even once during this entire process, and he can trust that he is viewing a genuine and untampered version of the student's credential.

The final prototype, CryptoCert, was hosted on <https://edu-blockchain.herokuapp.com>, and all the code can be found at <https://github.com/varun27wahi/educhain>. It satisfied all our major requirements. It will be compared with the other implementations in the next section. We end this section by showcasing a few screenshots of the final prototype in figures 8, 9, 10.

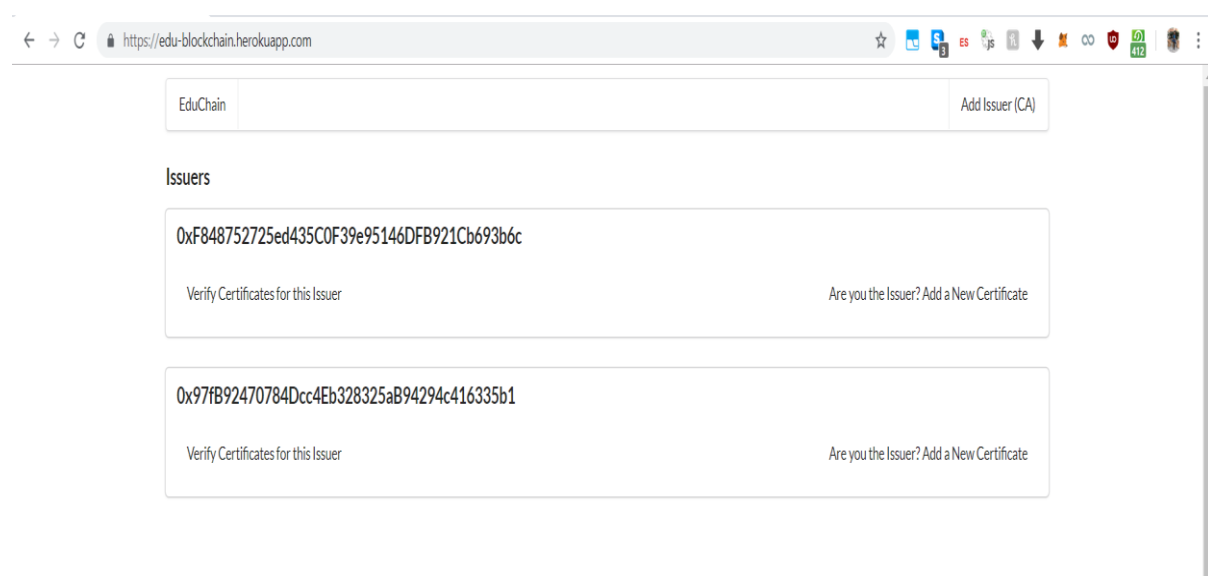


Figure 8 - The Home Page

← → ↻ https://edu-blockchain.herokuapp.com/issuers/0xf848752725ed435c0f39e95146dfb921cb693b6c/certificates/new ☆ [Icons]

EduChain Add Issuer (CA)

Issue a New Certificate for VIT University

Description

Issuing Authority

ID of Recipient

Type of Certificate

Additional Details

[+ Issue to Blockchain](#)


 Unique ID of this Certificate

Figure 9 - Issue a New Certificate

← → ↻ https://edu-blockchain.herokuapp.com/issuers/0xf848752725ed435c0f39e95146dfb921cb693b6c/certificates/verify/0 ☆ [Icons]

EduChain Add Issuer (CA)

[Back to List](#)

Verify Certificate for VIT University

Property	Value
Unique Certificate ID	44780778696187182796342965305237075805660540544968639802287678410790100132426
Description	Ethereum Course
Issuing Authority	VIT Blockchain Club
Recipient ID	15BIT0102
Issuing Date	Friday, April 5th, 2019, 1:59:53 AM
Type of Certificate	Course Completion
Additional Details	Grade: S


 **How to Verify!**
To verify the certificate, match the ID given here to the one given by the student.

Figure 10 - Verifying a Certificate

6 Results

In this section, we compare how our prototype, CryptoCert stacks up against the other implementations. We will also discuss about the monetary charges for implementing this system on the Ethereum blockchain.

6.1 Comparison with Other Implementations

We decided to compare the major implementations based on five different parameters in Table 1.

- **Integrity and Proof of Existence:** These are the two major features guaranteed by the use of blockchain, which make the entire idea possible. They ensure that the certificate exists, and has not been tampered with.
- **Universal:** This parameter looks at whether the current implementation can be extended to all the issuers or to different documents (such as transcripts or degrees).
- **Approving Authority:** This parameter compares if the implementation has a central issuing authority which will approve issuers before they can start issuing credentials to the students.
- **Hash or Credential? (H/C):** This parameter compares if the entire credential is being uploaded to the blockchain, or only the hash of the document.

Table 1 - A Comparison between the different Implementations

	Integrity	Proof of Existence	Universal	Approving Authority	Hash or Credential? (H/C)
Blockcerts [14]	✓	✓	✓	✓ *	H
University of Zurich [19]	✓	✓	-	✓	H
Brazil HEIs [20]	✓	✓	-	✓	C
KUDOS [18]	✓	✓	✓	-	-
Lifelong Learning Passport [9]	✓	✓	✓	-	H
CryptoCert	✓	✓	✓	✓	C

* *partially met the requirement*

[19] and [20] did not satisfy the *Universal* parameter as the [19] system was implemented just for that particular university, with only their employees eligible to use the system; and [20] is again fully dependent on the Brazilian Public Key Infrastructure, and therefore mostly useful for Brazilian HEIs.

[18] and [9] do not mention the use of a central issuing authority in their proposals. Blockcerts [14] does not have a central issuing authority, but does allow for the student to confirm the issuer's identity before getting the credential issued.

[18] is unique in the sense that it does not give any concrete implementation. The main aim of the paper is to propose the idea of the intellectual currency, Kudos, as discussed in section 3.

Apart from our implementation, only [20] have planned to upload something other than the hash of the document to the blockchain. In particular, in the *Diploma* smart contract of their proposal, a *diploma struct* with core details about the diploma is being uploaded to the blockchain. We can conclude from the comparison that our implementation is the only one that satisfies all our elicited requirements completely.

6.2 Cost Analysis

In this section, we are going to explain the concept of *gas* in Ethereum. In section 2, we've already seen how processing every new transaction to the blockchain takes a decent amount of time and money in the form of electricity, which is used to solve the complex cryptographic puzzle in order to mine the block (and make the transaction valid in the process).

Consequently, a malicious user could easily overpower and spam the network by creating or using smart contracts that contain code which require a lot of computational power to run and execute. In doing so, he will waste a miner's precious resources which should instead have been used for mining genuine transactions that are essential for the functioning of a blockchain.

To preclude such a scenario, the developers of Ethereum introduced the idea of gas. Each trivial operation that is being executed by a smart contract (in the form of an OPCODE), be it simple addition and subtraction, all the way up to finally broadcasting a transaction, costs an amount of gas to the user. An example of the exact amount of gas charged by the EVM to carry out certain operations is given in Table 2.

Table 2 - Gas costs for some Trivial Operations

Value	Mnemonic	Gas Used	Subset	Removed from stack	Added to stack	Notes
0x00	STOP	0	zero	0	0	Halts execution.
0x01	ADD	3	verylow	2	1	Addition operation
0x02	MUL	5	low	2	1	Multiplication operation.
0x03	SUB	3	verylow	2	1	Subtraction operation.
0x04	DIV	5	low	2	1	Integer division operation.

Therefore, each and every transaction issued by the user towards the smart contract costs him a certain amount of gas. This total amount of gas is multiplied by another variable, known as the “gas price”, to get the final cost in ether that the user has to pay in order to successfully complete the transaction. Gas price is the price per unit gas that the user is ready to pay in order to add his transaction to a block. The higher this price, the quicker and surer the block containing the transaction is mined to the blockchain. The gas price is normally specified in *Gwei*, which is approximately 10^{-9} ether.

The total costs for running each of the functions in our particular smart contracts were calculated, and the results are summarized in Table 3. As we can see, the costs are very minimal, and won't affect the current functioning of things in anyway. Most importantly, the issuer will not have to charge students extra to avail this facility. When we consider all the time and money that will be saved by replacing current systems with the proposed one, the issuer stands to instead make a large profit, and can sanction the extra money to more pertinent issues. Note that a user usually pays a gas price of 2 Gwei to balance between the need to get the block mined quickly and expense.

Table 3 - Cost for each Operation (\$)

Operation	Cost	
	At gas price of 1 Gwei	At gas price of 2 Gwei
Creating the Central Authority	22 cents	45 cents
Adding a New Issuer	19 cents	40 cents
Issuing a New Certificate	5 cents	10 cents

7 Discussion and Future Work

7.1 Discussion

The prototype CryptoCert satisfied all our requirements as discussed in section 6.1. Most importantly, we were able to achieve academic credential verification without involving any third party (e.g. the issuer, or a notary). This is a major improvement over the traditional system of issuing and verifying academic credentials.

If implemented, our proposed system would bring about the following benefits for our stakeholders.

- For the student, getting his credentials issued to the blockchain would save him a lot of time and money. He will not need to contact the University repeatedly to get his transcripts sent to a potential university or employer. He also would not have to pay for multiple copies. He will also have control over his achievements, and a lifelong indestructible record/proof of work.
- For the issuer, using the blockchain will save them thousands of dollars in printing and administrative costs. Each document needs to be generated only once. Moreover, they won't have to deal with hundreds of queries each day from verifiers, asking them to confirm a student's degree or transcript. This will save them tons of money and overheads.
- For the verifier, hours of time spent verifying each and every detail of hundreds of employees will be saved. There will also be no need to contact the original issuer to verify academic credentials.

7.2 Future Work

The next logical step to our proposal would be to develop, for each student, a life-long learning passport as proposed by Gräther et al [9]. The main idea behind this is to have a single document of sorts for each student, that keeps a track of all the student's achievements till date. This includes not just formal degrees or transcripts, but also MOOC (Massive Open Online Course) certificates, informal skill endorsements, badges, approval ratings, and so on.

By doing so, students will have a permanent record of all their lifelong achievements. Also, they will not have to depend on the original issuer to get these records validated for a verifier, since they will be stored on the blockchain. Because of this, even if the original issuer is destroyed, goes bankrupt, or the student moves to another country, he will never

have to worry again about losing these important credentials. They will act as his proof of achievement all over the world.

Lastly, our prototype could be improved in numerous ways. For example, we could add a search bar that the verifier can use to find a particular certificate, instead of manually going through the list of certificates in the table of a particular issuer. However, as mentioned before, this prototype was just built as a proof of concept, and was not the main goal of this paper. These issues can be improved on before deploying a production-ready solution.

8 Conclusion

In conclusion, we proposed and tested a new system, CryptoCert, for the issuing and verification of academic credentials. In doing so, we discussed in detail exactly how using blockchain technologies in any domain today can revolutionize all sectors and industries. In particular, we demonstrated how all the unique qualities of blockchain can be successfully harnessed to revolutionize the education sector.

The system we proposed has innumerable benefits over the traditional paper-based system for issuing important academic documents. Not only that, we also discussed how our blockchain-based solution beats even the more modern digital certificates system in terms of, but not limited to, security, efficiency, as well as disintermediation. This is explained in much more detail in section 2.4 and 2.5. Finally, we have successfully demonstrated how using blockchain to remove the need of a third-party for the purpose of verification leads to a tremendous amount of time and money saved, which can be used instead in improving other major flaws in the current education system.

Our study has described all the details of a proposed system, so that it can be used as a platform to disrupt traditional issuing systems, and give the power of achievement back to the learners.

Acknowledgements

Aswani Kumar Cherukuri sincerely acknowledges the financial support from the Ministry of Human Resource Development (MHRD), Govt. of India, under the research grant: SPARC/2018-2019/P616/SL under the SPARC scheme. Also, he acknowledges the financial support from Vellore Institute of Technology under the VIT SEED Grant.

References

- [1] (2018, January 1). India To Stamp Out Degree Fraud With Blockchain Technology. NewsBTC. Retrieved May 17, 2019, from <https://www.newsbtc.com/2018/02/06/india-stamp-degree-fraud-blockchain-technology/>
- [2] Pandey, N. (2017, March 21). Students, Beware: 23 Universities, 279 Technical Institutes In India Fake. Hindustan Times. Retrieved May 17, 2019, from <https://www.hindustantimes.com/education/23-universities-279-technical-institutes-are-fake-delhi-tops-list/story-EqeyFblUDKphKvT2tdrvjI.html>
- [3] Børresen, L. J., & Skjerven, S. A. (2018, September 14). Detecting Fake University Degrees In A Digital World. University World News. Retrieved May 17, 2019, from <https://www.universityworldnews.com/post.php?story=20180911120249317>
- [4] Mthethwa, S., Dlamini, N., & Barbour, G. (2018). Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents. Retrieved May 17, 2019, from 10.1109/iconic.2018.8601200
- [5] Husain, A., Bakhtiari, M., & Zainal, A. (n.d.). Printed Document Integrity Verification Using Barcode, 70(1). Retrieved May 17, 2019, from 10.11113/jt.v70.2857
- [6] Zaiane, O., Nascimento, M., & Oliveira, S. (2002). Digital Watermarking: Status, Limitations and Prospects, 02-01. University of Alberta. Retrieved May 17, 2019, from <https://web.archive.org>
- [7] Eldefrawy, M. H., Alghathbar, K., & Khan, M. K. (2012). Hardcopy Document Authentication Based on Public Key Encryption and 2D Barcodes, (2012 International Symposium on Biometrics and Security Technologies), 77-81. Retrieved May 17, 2019, from 10.1109/isbast.2012.16
- [8] Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. Publications Office of the European Union. Retrieved May 17, 2019, from <http://publications.jrc.ec.europa.eu/repository/handle/JRC108255>
- [9] Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). Blockchain for Education: Lifelong Learning Passport, 2(10). European Society for Socially Embedded Technologies (EUSSET). Retrieved May 17, 2019, from <https://dl.eusset.eu/handle/20.500.12015/3163>

- [10] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin. Retrieved May 17, 2019, from <https://bitcoin.org/bitcoin.pdf>
- [11] (2016, January 1). Sony Global Education Develops Technology Using Blockchain For Open Sharing Of Academic Proficiency And Progress Records. Sony. Retrieved May 18, 2019, from <https://www.sony.net/SonyInfo/News/Press/201602/16-0222E/index.html>
- [12] Zhang, Z. (2017). US Patent, (US20170346637). Retrieved May 18, 2019, from <http://www.freepatentsonline.com/20170346637.pdf>
- [13] Boeser, B. (2017, July 24). Meet TrueRec By SAP: Trusted Digital Credentials Powered By Blockchain | SAP News Center. SAP. Retrieved May 18, 2019, from <https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/>
- [14] Durant, E., & Trachy, A. (2017, October 1). Digital Diploma Debuts At MIT. MIT. Retrieved May 18, 2019, from <https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>
- [15] (2019, January 1). University Blockchain Experiment Aims For Top Marks. CNN. Retrieved May 18, 2019, from <https://edition.cnn.com/videos/tv/2018/06/28/blockchain-university-dubai-global-gateway.cnn/video/playlists/global-gateway/>
- [16] (2018, September 21). Calicut University Plans To Utilize Block Chain Tech For Academic Records. The Times of India. Retrieved May 18, 2019, from <https://timesofindia.indiatimes.com/city/kozhikode/cu-plans-to-utilize-block-chain-tech-for-academic-records/articleshow/65892634.cms>
- [17] (2017, January 1). DFIN 511: Introduction to Digital Currencies. University of Nicosia. Retrieved May 18, 2019, from <https://www.unic.ac.cy/blockchain/free-mooc/>
- [18] Sharples, M., & Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward, 490-496. Retrieved May 18, 2019, from 10.1007/978-3-319-45153-4_48
- [19] Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S. S., & Stiller, B. (2019). The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling, 185-196. Retrieved May 18, 2019, from 10.1007/978-3-030-04849-5_16

- [20] Palma, L. M., Vigil, M. A. G., Pereira, F. L., & Martina, J. E. (n.d.). Blockchain and smart contracts for higher education registry in Brazil. *Int J Network Mgmt*, e2061. Retrieved May 18, 2019, from 10.1002/nem.2061
- [21] Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (n.d.). A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry*, 10(10), 470. Retrieved May 18, 2019, from 10.3390/sym10100470
- [22] Zhu, L., Wu, Y., Gai, K., & Choo, K.-K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. *Future Generation Computer Systems*, 91, 527-535. Retrieved May 18, 2019, from 10.1016/j.future.2018.09.019
- [23] Yang, M., Zhu, T., Liang, K., Zhou, W., & Deng, R. H. (2019). A blockchain-based location privacy-preserving crowdsensing system. *Future Generation Computer Systems*, 94, 408-418. Retrieved May 18, 2019, from 10.1016/j.future.2018.11.046
- [24] Anand, A., McKibbin, M., & Pichel, F. (2017, May 2). Colored Coins: Bitcoin, Blockchain, And Land Administration. Cadasta. Retrieved May 18, 2019, from <https://cadasta.org/resources/white-papers/bitcoin-blockchain-land/>
- [25] Vitalik Buterin. 2014. Ethereum: A next-generation smart contract and decentralized application platform. Retrieved May 18, 2019, from <https://github.com/ethereum/wiki/wiki/White-Paper>
- [26] (2018, January 1). ethereum/eth-hash. Ethereum. Retrieved May 18, 2019, from <https://github.com/ethereum/eth-hash>
- [27] Bartolomé Pina, A. R., Bellver Torlà, C., Castañeda Quintero, L., & Adell Segura, J. (n.d.). Blockchain en Educación: introducción y crítica al estado de la cuestión. *EduTec-e*, (61), 363. Retrieved May 18, 2019, from 10.21556/edutec.2017.61.915 (English version)
- [28] Turkanovic, M., Holbl, M., Kotic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEE Access*, 6, 5112-5127. Retrieved May 18, 2019, from 10.1109/ACCESS.2018.2789929
- [29] Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.*, 5(1). Retrieved May 18, 2019, from 10.1186/s40561-017-0050-x

[30] Dimitrov, D. V. (2019). Blockchain Applications for Healthcare Data Management. *Healthc Inform Res*, 25(1), 51. Retrieved May 18, 2019, from 10.4258/hir.2019.25.1.51

[31] Yakovenko, I & Kulumbetova, L & Subbotina, I & Zhanibekova, G & Bizhanova, K. (2019). The blockchain technology as a catalyst for digital transformation of education. *International Journal of Mechanical Engineering and Technology*. 886-897. Retrieved May 18, 2019, from <http://www.iaeme.com/ijmet/issues.asp?JType=IJMET&VType=10&IType=01>