**Abstract**

This paper introduces our study on applying Blockchain Technology to education. It includes a comparison of two selected project on same matter in order to give an idea about ongoing studies of block chain applications for education. It continues with some problems on the current systems.

In this paper we described our approach to the problems and the technology used in first release of our app, CertIst: an app built by a team from Bahcesehir University (Istanbul) to give a support to many efforts for blockchain applications on registration and verification of – widely speaking - authentic document and more specifically on education area such as diplomas and transcripts.

**Introduction**

Individuals are turning to be a giant mass of information such as past records, job experiences, registries, certificates and diplomas as a necessity of a world running to be more sophisticated, fast and global. Thus, such information becomes dramatically important and valuable and therefore commercial. Further, any information is not isolated from the aggregated huge poll of information: An authenticated diploma is nothing but a piece of paper if issuer of such diploma is not authenticated and authorized by verifier. The fact that we try to emphasize above, itself, built a very complex and extremely costly bureaucracies which incompatible and generates an international bureaucracy which is further complex and costly. Below, we briefly introduce main causes of ineffectiveness of traditional ways to handle our problem and how a new technology, blockchain may give us an opportunity to do the same task as better yet.

**Time Management**

One of the main struggles that we are facing everyday is the time management. Over the last decades many innovation occurred rapidly and it is getting harder to follow them as time passed. It causes a time inefficiency problem for the institutions more than it ever was. On the other hand the improvements in each industry necessitate new skills and qualifications from participants of work. It is not just an immutable challenge for the firms in private sector due to market competition, but also a need for effective allocation of human (not just) resources.

Necessity of many qualifications in a competitive ambient, enforce students to have to be both successful with their majors and also to gain more skills and make their selves better candidate to be hired by firms.

Traditional mechanism to hire new employees is far to be efficient beside such hard task of reproduction and allocation of human resources. Today, the unique tool to verify a candidate’s diploma for a firm is to contact the school and ask diploma’s authenticity with its registration id. Since there are many different candidates for firms and schools have lots of graduates who are currently looking for a job, this solution requires a lot of time and work.

[**Counterfeiting**](http://tureng.com/tr/turkce-ingilizce/counterfeiting)

Fraudulent activity on academic credentials is a yet another problem. There is a fake diploma industry across the globe. Many websites are providing fake diplomas in return of a relatively small amount of money for their customers. Holding the question marks of opportunity gap to gain a verified diploma and its sufficiency alive, we can clearly suggest that such fact at least worsen unfair and ineffective election of valuable resources. We should also consider that those jobs include not just CEOs but engineers, doctors, teachers even ministers or presidents.

**Blockchain**

Recent developments in the software technology provided us not the perfect solution but a promising path as we deeply dive into Blockchain technology. Without a doubt, the current system has multiple flows when it comes to issue, verify and share document of achievements, this is not only causing great mistrust to the system but also costs academic institutions and corporations none negligible share of funds per year. Blockchain technology provides us a unique opportunity to design more efficient systems with better security solutions which benefits and gives more autonomy to the individual and the other parties involved in the process.

Application of Blockchain’s Decentralized Encrypted Technology into CertIst, gives us an opportunity to solve this problem with a better mechanism. With this new system schools can be sure that it is impossible to make an imitation of their valuable diplomas and their graduated students can easily share a single links with others or firms; with whoever wants to access their diploma. Companies can easily access candidate’s qualifications in seconds without a need of a mediator.

**Descriptive Analysis**

There are many implementations of blockchain technology for certificates by both academy and for profit organizations. From where we stand, one or few institutions implementing this technology will not be able to provide a solution to the problem at hand. In order to achieve an efficient solution, it is essential for institutions to cooperate and reach somehow a consensus which can be implemented globally (or at least regionally for the time being) and recognized by authorities.

Efforts to digitalize documents of achievements by using Blockchain technology will revolutionize the industry in many ways for sure. Current certification mechanism is way behind its potential and lack technological improvements. With Blockchain Technology it is possible to add immutability, accessibility, authenticity and more features to the system desired to be designed.

Existing projects on concerned matter vary from each other with simple design decisions made in the early stages of development process, which causes a snowballing effect by the delivery of the final product. That’s why every decision needs to be considered carefully with respect to the history of “blockchainification” the certificates.

First milestone was the “Blockcerts” project developed by Massachusetts Institute of Technology. The project has an effort for a more noble cause; to achieve an open standard in the Blockchain Industry. That’s why any institute is welcomed to join their platform and issue their documents of achievements with using Bitcoin and Ethereum Blockchain.

Though the academic projects took the lead at current researches of blockchain based certification, it is followed by some private companies. Here below we briefly listed some prominent projects.

**Existing Projects**

* + In October 2017 [MIT](http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017) announced they gave Digital Diplomas to 111 of their new graduated students. They used an app called Blockcerts to verify diplomas for MIT’s graduated students. MIT’s project was the pioneer on using blockchain technology for education.
  + In June 26th2018, Russian Financial University announced that they will store diploma records using blockchain. They are using their website to verify diploma’s authenticity with diploma number.
* There are some private companies in many countries including Turkey, who are trying to sell their blockchain diploma service to schools as a product. They may charge their customers with their own tokens or with traditional currencies for each diploma issued.
* Echolink and BCDiploma are two examples of private enterprises in such sector.

Below, we report our comparative analysis between two projects: BlockCerts as a project from Academia and Echolink from private sector.

**Comparative Analysis**

In both of the projects is possible to issue batch of documents and achieve privacy with hashing.

For final users there is not much difference. Both services can be accessed through web while Blockcerts already offers a mobile supports for their users. It seems like Echolink is planning to add a mobile support in the future and also a “Dynamic Blockchain Browser” which offers improved user experience according to their claim.

One of the main differences occurs when it comes to revocation of the documents. Blockcerts makes it possible to revoke the document of achievement after its issued and written to the chain by putting a flag to the corresponding transaction, there is no possibility of revocation on Echolink’s platform.

Since another difference, is about verification. The algorithm being used by Blockcerts is more sophisticated when compared to Echolink. For Echolink once a document of achievement is uploaded it is assumed verified. Blockcerts uses multiple steps to verify the document by checking transaction information, issuer’s identity, revocation information and more.

Blockcerts is an open project and has a community about development issues while Echolink is totally private.

Blockcerts and MIT Media Lab provide useful and helpful documentations. Echolink lacks of information.

Echolink uses Oracles to guarantee safety and transparency of commercial transactions while there is no need for it in Blockcerts.

Echolink claims that their structure is chain agnostic (means it runs on various platforms), however the first implementation works only on Ethereum Blockchain and future developments will include Neo, Dash and IOTA. It will be a huge challenge for them to implement this technology to these various platforms as we know the fundamental flows in some of these platforms causes even a basic transaction to fail. Blockcerts instead works on Bitcoin and Ethereum environments but simultaneously necessitates both of them due to the business logic of their product.

Blockcerts focus on diplomas and academic certificates. Echolink declared that they don’t just provide services on diplomas; but also for working records, financial records and checks.

Echolink has a token in crypto-currency market and their market-cap was 1.930.000 [USD](https://www.coindigital.com/what-is-echolink-eko/) when we wrote this whitepaper. Since Blockcerts is an academic project, they don’t have any.

The most distinctive difference about these two projects is Echolink is a paid service provided by third party while Blockcerts is more like a community driven project to standardize this system between institutions, and only cost on this project is the mining fee paid in the process of issuance of the documents.

**Approach**

**Verbal Description**

The implementations which are carried out by for-profit organizations are nothing but selling the hype caused by Blockchain. They are just business models and have no academic purpose or background which we cannot benefit remarkably. On the other hand, research conducted by Massachusetts Institute of Technology and University of Nicosia provides us great amount of information during our research process, which fundamentally shaped our approach to the problem. After careful considerations, we have decided to implement blockchain certifications in various platforms, starting with Ethereum.

In our system, we provide a blockchain wallet for our graduates and make them able to share link of their diplomas for their job applications or in any online platforms such as LinkedIn, so the firms that they apply to work with, can easily verify their diplomas authenticity.

In order to teach firms how to use this new technology, we started to reach to many firms in different sectors. Having 500 CO-OP partners in many different sectors, Bahcesehir University gave us an opportunity to start up very fast. We contact them to teach how they can use our system efficiently so firms can understand this technology better and use it without any doubts. We try to get through this transitional period as fast as we can, in order to realize the advantages of blockchain diplomas for everybody, starting from our graduates.

**Technical Description**

In our very first prototype we kept things as simple as we can to deliver and start to utilize the product.

Certist is composed of a 3 components.

1. Backend API

The backend API is mainly used to retrieve and write data on the Ethereum block chain.

2. Frontend

The frontend handles interactions with the backend and the user interactions with the Certist app.

3. Smart Contract

Our Ethereum Smart contract is the mechanism that is used to store and verify diplomas and certifications on the block chain.

The system works as it follows:

The user’s cryptographic keys are generated when the app is launched for the first time, then encrypted and safely stored in the device for later use. The key generation seed is then displayed so users can create a safe backup in case of a loss of keys or devices. Such process is provided by MetaMask.

Via a simple panel the issuers issue the diplomas by creating an Ethereum transaction and writing the necessary data into it. The data is stored in the contract. Some smart contract functions can only be called by specific keys; this is designed so that only verified issuers are able to issue new diplomas or certificates.

Afterwards a request get sent to the smart contract which triggers the write function, an Ethereum transaction is broadcasted to the network from issuer’s public key to student’s public key. The documents are uploaded to a decentralized storage platform (IPFS). Once it is uploaded, IPFS generates a hash automatically, which uniquely identify the document. The hash is then written to the contract.

When the certification is desired to be shared, a link gets generated which redirects the user to the verified document page where the PDF file is shown.

Verification process is also a simple request to the contract which compares the return values from the contract’s related function with the original ones.

A simple code snippet for verification of authenticity is shared below:

addresspublicowner;

functionowned() {

owner = msg.sender;

}

modifieronlyOwner {

if (msg.sender != owner) throw;

\_;

}

On frontend all can be done through the QR code or permalink provided by the Certist app for every certificate the user has. Verifiers can see the relevant information that confirms the issued diploma or certificate is genuine and authentic. Any certificate can be retrieved by calling the smart contract upon request.

**Further Research**

As we intended to carry out future research on this subject, it is possible for us to experiment with different blockchain platforms as we know perfect solution does not exist. Yet Bitcoin implementation remains to be a question since there are several working examples.

It is our intention to cooperate with different institutions to provide a use case of blockchain which can be adopted globally.

Our scope is not moving Bahcesehir University’s diplomas to blockchain. We want to build a Blockchain Ecosystem between universities and institutions starting from Turkey. That’s the main reason why we are publishing our code open source for further researches. We want other universities to cooperate with us to work on this technology. So, we can apply this technology better between all of the universities and institutions.

Another problem that we study on is decentralization of authentic documents. Migrating them to a public blockchain system is a step for sure but still too far to speak about fully decentralized future of certification ecosystem for two main aspects:

1. Verification processes are too strict to universalize. While each national central institutions determines authentication criteria of the documents, creating universal validation mechanism for blockchain certificates in a fast and economic manner remains as a hard and long task.
2. Current technologies on the topic includes CertIst have hybrid validation process where central institutions and technologies are still involved which always can create a thrust issue.

We consider some different business logics for CertIst, where always more information nodes - such as data of grades of each course for validating a diploma’s graduation grade, each grades from each exams, professor’s identifying information and more - are transferred to blockchain ecosystems and the requested piece from data pool can be validated inside the system.

Further, new business logic to demolish any authorization privileges can need to be implemented. Current authorization mechanism can create a thrust problem of issuers’ purposes. Sharing the authority of certificate issuance into the ecosystem by any user, seems to resolve the problem while it costs to the verifiers to keep and update a list of trustworthy issuers.

**Team**

**Cenk Şimşek**

Graduate Student in Bahcesehir University (Istanbul), Fin-Tech

Graduate Student in Istanbul Technical University (Istanbul), Economics

Java Developer

gibi.

Bu kısım anladığım kadarıyla whitepaperlarda önemli. Ekiptekiler hakkında tek tek isimler ve küçücük de olsa bilgiler eklenirse daha şeffaf, güven verici ve ilgilileri hakkımızda isterlerse araştırma yapmaya müsade eden bir şekle giriyor.