Towards an IPFS-Blockchain based Authentication/Management System of Academic Certification in Western Balkans

E. Leka*, E. Kordha** and K. Hamzallari*
* Polytechnic University of Tirana, Tirane, Albania
** University of Tirana, Tirane, Albania
elva.leka@fgjm.edu.al, ermelindakordha@feut.edu.al, kladji369@yahoo.com

Abstract - This paper presents an implementation which uses decentralized technologies such as blockchain and IPFS on the issuance and management of the academic certificates. The focus is on improving the actual process, as well as increasing integrity and trustworthiness of ownership of those certificates. The prototype we have developed is called BCert and its purpose is to add the certificates to blockchain network and to offer the possibility to verify them and make accessible to the potential stakeholders. It will also be used to verify that it is possible to upload a minimum of 32 certificates at one time and to evaluate speed of upload. BCert will aim to make the deployment and verification of those certificates quick, fast, secure, and efficient. It uses IPFS (Interplanetary File System) to have private logs and to increase efficiency. Additionally, based on the Technology Transfer concept, we predicted a model related to the launch of the technology to the market. The study was conducted online with 421 responses chosen randomly from several public and private universities in Albania and in Western Balkans.

Keywords – blockchain; IPFS; academic certificates; Solidity; Ethereum

I. INTRODUCTION

Traditional education institutions are based on a centralized system, where credentials and academic certificates are stored on a single location owned by a higher institution or a university. Therefore, the traditional way how those certificates are issued and verified may have some drawback such as: corruption, lack of transparency, falsification, being time consuming, reliance on third parties, and high cost [1,2].

Furthermore, actual systems are not made to handle large amounts of parallel requests and lack integrity of data stored. One example would be the downtime during a DDoS attack, or temporary (maybe even permanent) loss of data due to attacks, viruses and errors, or even human errors [3].

Another issue is the integrity of data stored and transparency, where digital access to the certificate is often missing. A basic example would be the digital verification of an ownership certificate. Usually, such certificate is issued as a hard copy, and signed by respective authorities. Although it might be hard to falsify such a certificate, someone who owns the right tools and purpose can certainly do this in mass. Finally, even though a falsification might be distinguished at a later time, it will spawn the tedious process of reevaluation taking years to undo the damage that has been made.

Due to its main characteristics such as: decentralization, immutability, transparency, being open source and anonymity [4,5], blockchain will help us to improve security issues and efficiency. Our proposed system BCert [6], is implemented in Ethereum platform network and smart contracts are deployed in Solidity language [7]. Additionally, IPFS (Interplanetary File System) is used to store the encrypted certificates [8].

BCert will increase efficiency of academic certificate’s issuance, because of the main features of blockchain such as authentication, certification, traceability and provenance. The implementation has 3 main roles: (1) The issuer institution, which main responsibility is to issue certificates with the appropriate student’s information; (2) The accreditor, which responsibilities are to add/remove universities and validation of the certificates; (3) An employer, which can verify if a certificate is valid and issue verified employment/title review records [6].

The private key of the accreditation body is used to accredit a university and on the other hand, the issuer university sign the certificate with its private key to assure that it is issued by a trusted authority. A potential stakeholder checks certificate’s authority by using the unique serial number of graduated student [9].

The paper is organized as follows. Section II presents the background and related work. The architecture of the system and its components are described in section III. Performance testing of the BCert’s system is presented in section IV and its potential business is discussed in section V. The conclusions and benefits of using BCert are presented in the last section.

II. BACKGROUND AND RELATED WORK

A. Background

The implementation of the project requires the use of different technologies such as: smart contracts, IPFS, PWA.
Ethereum [10] is a public permissionless blockchain platform that allows anyone to build and use decentralized applications that run on blockchain technology. Ethereum requires to use a consensus algorithm, which may be: PoW (Proof of Work), PoS (Proof of Stake), PoB (Proof of Burn), Practical Byzantine Fault Tolerance Algorithm, DPoS (Delegate Proof of Stake) and PoA (Proof of Authority) [11-13]. PoW algorithm is expensive due to high computational power and high energy consumption. We have chosen Clique Proof-of-Authority, as a new consensus algorithm that some Ethereum testnet are implementing [14]. Ethereum Virtual Machine (EVM) [15], is the heart of Ethereum, which can execute the complex algorithm codes. The proof of the algorithm that Ethereum uses for the mining process is called Ethhash.

Solidity is an object-oriented programming language developed in 2014, somewhat similar to Java. With the use of Solidity, we would encounter a new definition which is a “smart contract”. The smart contract is a set of instruction that does certain actions depending on user input. They operate within the internal blockchain environment called EVM (Ethereum Virtual Machine), and it is where the contract will rest after its deployment [16]. EVM is an environment responsible for performing instructions. It is made of all the nodes of the blockchain, unifying instructions, operations, and storage of data across all the nodes into a single environment.

B. Web Apps & PWA

Even though blockchain is a powerful technology in itself, it cannot work without external help. In order to utilize this technology, one has to develop other tools which make it possible to transfer information from the user to the network in a safe, simple, and secure way.

In order to bring blockchain to current devices, we use PWA (Progressive Web Apps), which helps building user interfaces, making it easier to issue and verify certificates. Such apps will indirectly communicate with the blockchain, retrieving data form the network, and performing actions predetermined in smart contracts. These apps will serve as entry points to the project. A process would be the verification, scanning or issuance of a certificate. Usually, native applications are built that can be run on specific platforms, but this needs a lot of work for little benefits because we need to code separate apps for different platforms (Linux, Windows, Android, iOS) and in return we have better performance. This is inefficient in our case.

PWA is a new technology that offers specific platform operations, which are stable and can be installed. PWA is not a single technology, but rather a combination of other technologies, similar to a philosophy of building apps [17].

C. IPFS

IPFS is a way of including even more data into a certificate. It is based on a peer-to-peer protocol for data storage and retrieval on a distributed system. IPFS uses content addressing in order to find files. Similar to BitTorrent, data is distributed among peers (members of the network) and can be retrieving using DHT (Distributed Hash Table) [18].

IPFS is based on: (1) Content addressing; (2) Directed Acyclic Graphs (DAG); (3) Distributed Hash Tables (DHT). Content addressing is used to identify data based on content and not location. Usually on current systems content is found using locations.

D. Related Works

From our literature review, we identified many proposed solutions/implementations that use blockchain in education domain, but our focus is on those who propose blockchain to manage certificate/credentials/diploma distribution and verification [19]. Some of most well-known implementations include BlockCerts[20], UZHBC, SmartCert, EduChain [21], EduCTX, Cerberus and UNIC [22].

The first state that has adapted and deployed blockchain technology in education is Malta, which has implemented, and open-source platform called BlockCerts [23]. This decentralized system is used mainly to issue, manage, and verify the certificates [24]. Meanwhile, authors in [25] have presented another system named EduCTX, which proposes to use European Credit Transfer and Accumulation System (ECTS). It is implemented on the open-source Arc Blockchain Platform.

The University of Zurich has developed a verification blockchain based system in Ethereum platform which enables smart contracts for managements and verification of diplomas [26]. On the other hand, the University of Nicosia in Cyprus, has adapted blockchain in education not only to record students’ diplomas/achievements, but also to pay the fees by using Bitcoin [27].

Authors in [28] have developed a training certificate management system named CertificateChain, which provides a user experience and allows participants to manually submit their certificates in pdf format. Furthermore, they have evaluated the prototype’s feasibility and scalability.

Zhao et al. [29] have proposed a NFT-based certificate framework, called NFTCert, which enables the integration of NFT concept to prove legitimate certificate through a Blockchain network. The authors have described the implementation of NFTCert framework and argued that their proposed system improves the process of authentication, increase transparency, and offers confidentiality. The main benefit of their system is that a user has the possibility to keep all educational certificates records in an digital wallet.

In paper [30], it is described the PoC prototype implementation in Ethereum platform of as system that enables smart contracts in order to register/consult student certificates which are issued by a higher institution. Meanwhile, authors in [31] have presented their blockchain based system, which intend to offer a standard sharing platform to store, access and monitor various documents such as diplomas, government papers, transaction papers in order to avoid the problem of fake certificates.
Vidal et al. [32] have presented proof of concept of their CertEdu prototype, which main functionalities are to issue, revoke, share and verify the academic degrees. The authors have analyzed the benefits the technology could bring in certificates management and have also identified some problems that need to be resolved such as: unpredictability of the issuance costs, due to the limitations on predictions of transactions costs in long time in public networks such as Bitcoin and Ethereum.

Thus, as authors in their paper [33] argue, using blockchain in education domain will help to solve 4 main drawbacks of actual traditional systems of distributing and managing certificates as follows: (1) overcoming diploma’s counterfeiting; (2) reducing costs; (3) increasing efficiency in terms of time and energy; (4) impacting on increase the workers competence, thus producing qualified workers.

III. ARCHITECTURE OF THE SYSTEM

A. Architecture

This section presents the system architecture of our proposed solution (as it is shown in Fig. 1) and discusses in further details the deployment process.

![Overall Architecture of the System](image)

As can be seen, the entry point of our data would be on the front-end. This information will be manipulated and sent to the respective gateways. Depending on the information which has been classified prior to its initiation, it will be sent to the proper networks, IPFS or Blockchain. It should be kept in mind that not only the information encrypted using a private key, it is also encrypted via the HTTPS protocol through its journey on the internet. It is important to state that no encryption key is sent to the network. This drastically increases security, but also renders these data inaccessible in case the encryption key is lost. After it is sent to respective gateways, this information is separated, and each gateway sends the information to the network peers or nodes. In the case of IPFS it is stored directly on the network, whereas blockchain it is modified by a set of methods specified in the smart contract. It should be clear that information sent to smart contract is publicly visible and addressable.

B. Implementation

For implementation part of this solution is used Ethereum Platform. The Smart Contracts will be deployed in Solidity Language. Certificates will be saved encrypted on IPFS (Interplanetary File System). We propose two main roles: issuer and users. Issuers can: add credentials; view their credentials; issue credential to user. Users can: view the list of credentials they have received; make their credentials visible to another user; decide whether they want to make their credentials public or not.

It is not possible to add a certificate to the blockchain without the proper authority. The certificate would be considered valid, only if it is signed by issuer university or accreditation body.

Looking in more details in functionalities of proposed solution [9]: (1) University Interface, is part of the ecosystem for creating, signing and issuing certificates. It is responsible to send the data, distribute the passphrase and certificate details; (2) Verification Interface enables the user to check if the issued certificate is valid or not. The verification application follows all PWA standards and protocols; (3) Accrediting Interface, is responsible to add an accreditor to the system, and furthermore this accreditor can add other universities to the list. After this process, the university can add and deploy certificates on its own, by using unique identifiers such as name or other keys.

The system we have implemented, uses Ganache as deployment environment of smart contracts and Rinkeby as test environment. In [9], we have explained in further details how the system works:

1) The encryption of the data, which should be done before the transaction is created. It is important to save the encryption key locally and send it only to the graduated student [6,9];

2) The first node sends the signed transaction and broadcast it to the blockchain network;

3) The status of an academic certificate can be changed only by issuer university or accreditor.

C. Full Walkthrough Generating Certificates

Firstly, the university is required to configure the deployer with the configuration given by the network maintainers (accreditor or other entities). Then the form is required to be filled, containing the necessary student information, along with a photo ID of the student (mandatory). After that the information provided should be stored locally using the appropriate button and entering encryption key. The same step is repeated until all the students are processed (note, no more students than the recommendation can be stored).

![Filling student information and selecting photo ID](image)
A new section should appear, looking like in the figures below. Once finished, the deployer can export certificates using the “export” button as shown and store it somewhere safe in order to pass it to the signer (part of higher university staff). It is not recommended to transfer these files over the internet. Other methods such as internal network connections or USB transfers are recommended.

In order to deploy certificates, one needs to navigate to the correct panel and choose the exported file from the above steps. After that, a list of students should appear with their respective information. This information is verified and then deployed using the “deploy contracts” button. Then, the transaction is signed using the private key (from configuration settings) and after 15-20 seconds appears ‘Receipt Available’ on the console, indicating that the transaction has been successfully confirmed and the certificates successfully deployed.

By using IPFS in our system brings two main benefits. First, it would save storage on the blockchain network because the profile information will be stored externally. Secondly, while IPFS address is immutable, will provide proof of authenticity.

To verify the certificates, BCert offers two different ways. Fig. 3 shows the verification process by using the serial code. Meanwhile, another simplified method is to use the QR code as it is presented in Fig. 4.

Depending on the device, most likely the user will be prompted to allow camera access. However, this is not always the case, as in some devices this step is ignored, and camera access is granted automatically. Once camera access has been granted, the user needs to scan the QR code. If the scan is successfully completed, the student information should be shown.

IV. PERFORMANCE TESTING OF BCERT SYSTEM

In this section we observe BCert’s performance system, focusing on gas usage, as well as timestamp parameter for each transaction, in order to understand the computational and time resource requirements. The gas usage represents the operation’s complexity and there doesn’t exist any standard of converting gas to physical currency, but it depends on labour’s cost. The performance is evaluated by measuring: (1) the number of computational resources required to mine intermediate transactions, (2) resources needed to write, upload, access or update the academic certificates. We also intended to offer some parallelization to the BCert’s system. Till now, as Fig.5 shows, 32 academic certificates can be added in bulk, within 13 seconds.

![Figure 5. Evaluations of Paralelization (IPFS Impleted)](image)

We are using 2 servers conveniently named Nodeinit and Node2; each one running a different version of Linux in order to show that multiple systems are supported. Each server has 1GB of RAM and 1vCPU. Both servers are running 2 main nodes, Nodeinit is also running a bootnode. All four main nodes are running Geth client. By default, Geth does support creation of accounts within its command line interface, however it will be inconvenient to distribute these accounts to their respective entities. Fig.6 presents Server Tests – IPFS.

![Figure 6. Server Tests – IPFS (1GB RAM, 2.2 GHz)](image)

Server side is relatively flat. As seen, the first spike (around 12:40:00) on traffic is from the deployment of 30 images into the network. The second spike (around 12:42:14) is from a single certificate deployment. CPU and RAM are mostly unaffected from this type of action. Most changes in their graph are from internal OS processes.
V. BUSINESS POTENTIAL

In the previous sections, we presented all the benefits and advantages that the adoption of blockchain technology has in education domain, especially in academic certificates management. Any technology proposed to achieve some benefits for users, will have to go through an important process such as the Technology Transfer (TT) process. It is collaborative process between the inventor and an official Technology Transfer Office or agency or other institution taking the functionalities of such an office, during which the identification, protection, and commercialization of intellectual property occurs.

This process is related to the planned effort to enhance the movement of technology from a source to a potential user [34]. It is very important to study the human interactions when we want to understand what are the factors that impact the TT process [35]. The process of technology is very important since adoption of the new technology by users or by industry may be one of the limiting factors [36].

Based on the importance of the TT process identified by many authors of the field, the involvement of stakeholders interested in innovations and their concrete impact on the market, business, and economy, based on the functionalities of the proposed system, a study was undertaken on the main target audience which are students.

We conducted an online questionnaire with 421 responses, chosen randomly from several public and private universities in Albania and in Western Balkans. The aim was to understand some very important components that were supposed as core of the value proposition of the proposed blockchain system. Understanding customers, their needs, and the possible behavior of target audiences, is undertaken on only to help the Technology Transfer process in the near future, but also to seize the opportunities for further developing the functionalities of the system, as it should be taken to the market, to fulfill market needs.

By analyzing the responses of the questionnaire, we conducted that the audience (students in our case) should be better informed about main benefits the use of blockchain could bring to education domain. Thus, the promotion of the system is of great importance. More than 70% of students do not know about using blockchain in education. In the other hand, 65% of them are positive about using this kind of system that offers maximum data integrity and security. 43,1% are willing to pay through the online platforms. The other think that universities must invest in this technology and cover the costs. The cooperation with Education Institutions is highly recommended during the appropriate phase in the process of Technology Transfer.

Additionally, we analyzed the legal aspects of adapting blockchain in Albania and other Western Balkans countries. There is currently a positive situation regarding Distributed Ledger Technology (DLT) in Albania and Serbia, better than in all other Western Balkans countries. Advancement in legislation and proposals of legal acts is an opportunity for business development in Albania.

Even though we have identified some challenges. First, the licensing by National Agency of Information Service in Albania is required as a legal guarantee for the development of business in the field of DLT. Secondly, seeking permission for data storage as well as the duration of their storage within the meaning of the law requires an opinion to find the best solutions. Further legal assistance may be sought in the above cases.

VI. CONCLUSIONS

During the development of BCert prototype, we achieved: (1) a working user-blockchain interaction, (2) a sustainable and usable way of deploying certificates; (3) an overview on resources consumed; (4) a way to access certificates through multiple devices, such as personal computer, smartphone, smart TVs.

The proposed system increases value and time efficiency for the process of certificate issuance in education institutions, providing real time online verification, confidentiality, authentication, and revocation. We intend to offer parallelization of issuing certification. According to our testing results we can deploy 75 certificates for 15 seconds at the same time.

We analysed the business potential that BCert would have in Albania and Western Balkans. Even though, to fully adapt the benefits that blockchain technology could bring to education domain, the aspects of DLT legislation in Albania/Western Balkans, Intellectual Property, data protection and actors legally involved in the process need to be examined.

REFERENCES


