BCERT – A DECENTRALIZED ACADEMIC CERTIFICATE SYSTEM DISTRIBUTION USING BLOCKCHAIN TECHNOLOGY

Elva Leka, Besnik Selimi

Faculty of Contemporary Sciences and Technologies,
South East European University
e-mails: el23618@seeu.edu.mk, bselimi@seeu.edu.mk
North Macedonia

Abstract: In this paper we propose to use a blockchain based system, called BCert, which is used to store, distribute and verify academic certificates in order to improve efficiency and security. BCert is based on utilizing Ethereum smart contracts and leverages the benefits of IPFS (InterPlanetary File System), to store the certificates in a decentralized file system. Smart contracts provide a secure distributed and shared decentralized ledger of all assets and transactions. A cryptographic hash function shall be applied on document and result may be stored on a public blockchain in a transaction signed by private key of issuer institution which ensures the validity of documents. We intend to provide confidentiality to the data by encrypting them with AES encryption algorithm, before creating transaction.

Keywords: blockchain, certificates, smart contracts, solidity, AES, IPFS

1. INTRODUCTION

Problems we face today with academic degrees are backed by corruption, system flaws, ability to effortlessly falsify and distribute these degrees in large quantities are impractical ways to validate them if needed to do so [1-3]. Certificates which are issued in a traditional/physical way can be easily copied and their integrity and origin is hard to impossible to verify. Other issues are related to the way these certificates are issued, delays due to administrative level incompatibilities or miscommunication, credential transfers among faculties/universities.

Blockchain will be one of the next technology revolutions due to its main characteristics: no central authority, elimination of intermediaries, real-time settlement, drastic reduction in operational costs, high levels of transparency [4-7]. It can be applied in different domains such as: government [8], healthcare [9], finance, Internet of things [10], information security of energy internet [11], public and social services [12], reputation system [13] and education [14, 15, 16].

A variety of blockchain applications have been developed for educational purposes. Blockchain Technology will transform the education industry in different ways such as: certificate management, competencies and learning outcomes management, evaluating students' professional ability, protecting learning object, fees and credit transfer, competitions management, copyright management, interactions in e-learning, examination review and supporting lifelong learning [17, 18]. In this paper we are focusing on management of digital certificates. The current process for verifying an employee candidate's credentials can be very time-consuming, redundant and expensive, furthermore it may increase the chances for losing the best candidates to competitor companies based on the time delay. Blockchain can be used to issue unique digital assets that verify the credentials of academic degrees and certifications. This would make it much easier for potential employers to verify the degrees and save valuable time and money.

BCert, the solution we propose in this paper, uses concept of Blockchain and smart contracts to distribute and verify certificates. Blockchain can be implemented as: *(1) decentralized network,* in sense that there is no node that acts as the central server for the network, *(2) distributed network*, in sense that responsibilities are shared by the nodes. For the implementation of BCert is used Ethereum Platform network [19] and Solidity language [20] in order to deploy smart contracts. Certificates will be saved encrypted on IPFS (Interplanetary File System) [21].

The main roles of this implementation are: accreditation body, university, students and employer. Nodes on the network can issue and verify the credentials for any user on the network. A university is responsible for issuing certificates with the valid information, including student name, degree level, the title of the degree, year awarded, university, and serial number assigned by the system (which can be used as a unique identifier). An accreditation body can validate a certificate and an employer can issue verified employment/skill/title review records.

To check the authority of the certificate, the interested entity should use a unique identifier/serial number that is initially available to the Issuer University, accreditation body, student or employee. To assure that this certificate has been issued by a trusted authority, it must be signed with a private key, which is only available to the university and the issuing authority. On the other hand, the accreditation body uses its private key in order to accredit the university as well. When the university issues a certificate, it is automatically marked as valid/accredited and put into the network.

The paper is organized as follows. The next section presents related works in blockchain certificate distribution. In Section III is presented the proposed architecture of the system and how it works. The implementation design and testing are described at section IV and further development at section V. The last section discusses conclusions and benefits of using BCert platform.

2. RELATED WORKS

Many solutions have been proposed and developed from perspective of using blockchain in education domain. We limit our discussion to the systems and architectures that propose blockchain-based verifying and distribution of academic certificates.

Malta has become the first nation-state to deploy blockchain technology in education, issuing digital diplomas, training certificates and equivalency statements, using the BlockCerts standard [17]. BlockCerts is an open-source platform that is currently in development by Massachusetts Institute of technology (MIT), that mainly focuses on issuing and verifying official certificates using blockchain[18,22]. Blockcerts is based on the self-sovereign identity of all the participants by providing components to create, issue, view and verify certificates. According to our literature review, there are some other proposed solutions in this domain such as EduCTX, UZHBC (Unviersiy of Zurich BlockChain), EduChain, UNIC, Cerberus and SmartCert.

EduCTX [23] proposes a unified global higher education credit and grading system based on the European Credit Transfer and Accumulation System (ECTS), in which coins are transferred on the blockchain to signify academic study credits attained by students. It requires students and verifiers to maintain cryptographic credentials or digital identities to participate in the ecosystem.

UZHBC is a blockchain-based verification system, specifically for diplomas issued by the University of Zurich [24]. It uses the public Ethereum blockchain and employs a smart contract for both issuance and verifications, and accepts a PDF of the credential as input. It does not incorporate accreditation body. EduChain enables academic institutions to interface with blockchain infrastructure of trust. Educhain is building a series of solutions for academic institutions, such as enabling instant issuance and authentication of digital credentials, and a comprehensive “academic passport” of student achievements, using blockchain technology [25, 26, 27].

The University of Nicosia in Cyprus is also implementing blockchain technology as a way of recording students’ achievements [27]. UNIC is using Bitcoin Blockchain for many activities, such as fee payments, issuing academic certificates on Blockchain Technology and so on. It has commenced issuing all diplomas using the blockchain since 2017. To preserve the authenticity of the certificate, it uses the SHA-256 hash algorithm. Although UNIC does not offer a clear method of authenticity of parties and requirements for an employer to verify the certificate is inadequate.

At al. [28] authors propose a blockchain-based accreditation and degree verification system, called Cerberus. It uses on-chain smart contracts for credential revocation, and it does not entail students or employers to manage digital identities or cryptographic credentials to use the system.

Another blockchain based digital credentials verification platform is SmartCert [29], which is developed to establish the authenticity of academic credentials on a blockchain and to overcome the problem of fake certificates. SmartCert makes use of cryptographic signing of educational certificates to provide transparency in the case of recruitment. To verify the certificate, the student will share the hash with the prospective employer. However, SmartCert is vulnerable to attacks, has no clear method of authenticity of parties and need for basic information security measures [30].

If we consider authorization, the above mentioned solutions, do not provide many details on authorization theme. SmartCert claim they provide authorization in their solution, but there are not available any technical details. Also, the confidentiality theme is not ensured by the solutions.

In the system we propose, we provide confidentiality using AES algorithm before creating transaction and offer other certain features such as real time online verification, third-party verification, usability and revocation.

3. PROPOSED SOLUTION

In this study, it is aimed to verify and distribute digital certificates given to the students, by using Ethereum Blockchain based smart contract. Programming language that is used to deploy smart contracts is called “Solidity”. We have choose Solidity, because it is a well-established programming language used for coding smart contracts; other alternatives do not offer a stable and efficient environment.

The code written in Solidity is compiled and converted to bytecode and sent to the Ethereum blockchain as a Smart Contract.

The main roles proposed for BCert system are: *(1)* ***issuer***, which can be universities or training centers; *(2)* ***users***, which can be students, employers or academic institutions; *(3)* ***Accredication body***, which serves to validate the certificate. Uploading certificate to the blockchian is done only by issuers, who can: add credentials, view their credentials or issue credentials to user. On the other hand user can: view the list of their received credentials; make their credential public or not.

Once a certificate has been added to the blockchain, it can no longer be removed, and every activity regarding this contract is publicly available. Depending on how universities and accreditation bodies work together, a certificate can be verified at a later time, or upon its insertion into the blockchain.

3.1. Architecture of the system

The proposed architecture of the system is shown in Fig. 1. Certificates on a blockchain offer a wide variety of options and benefits. Authenticity of a certificate can be easily validated and tracked back to the issuing and accreditation body;

otherwise, the certificate is marked as invalid, although it will be almost impossible to insert a certificate without proper authority.

If accreditation body or university is later found to be fraudulent, all certificates issued by an accreditation body or university are later found fraudulent; all certificates issued by the former should be immediately invalidated. Furthermore any employer/company that employs such individuals can receive a notification if any of its employees belongs to the above group, but this depends on how the system will be implemented.

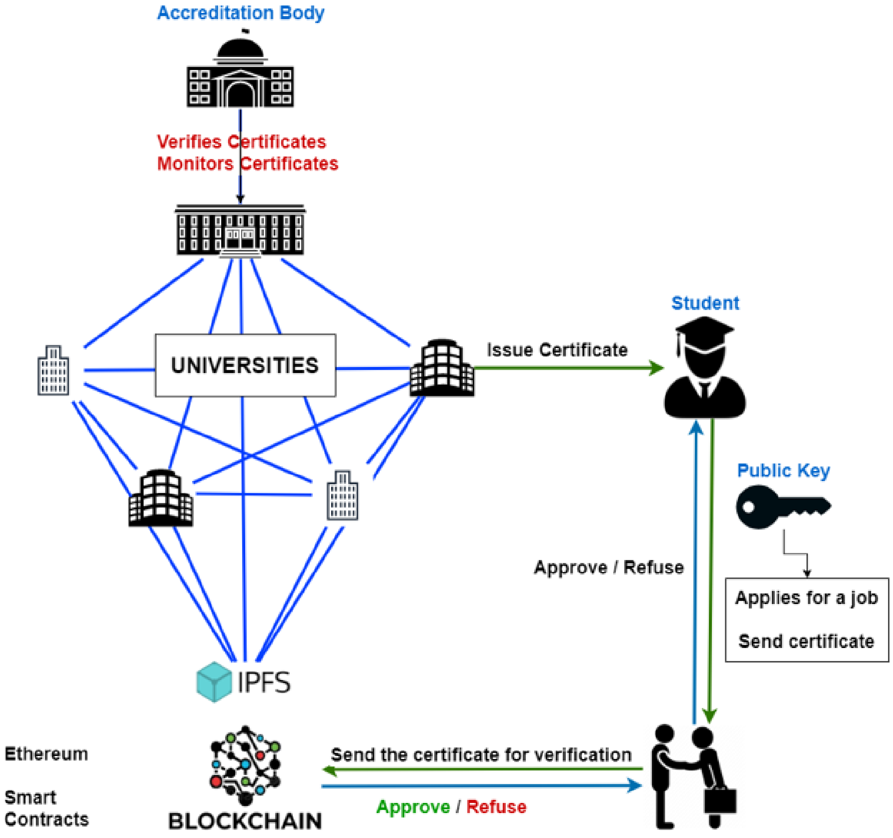


Fig. 1. BCert – Proposed Architecture of Decentralized Certificate Distribution

Moreover, there can be a second set of data, such as student ID, credits of each program, grades, which will be private and disclosed only with the students permissions. As a result there should be no additional recurring server or server management costs, as the information on blockchain is distributed among nodes connected to the blockchian. Although the aim is to have a serverless platform, depending on the final architecture, there might be a need for a simple low-cost server.

Having this platform depend on blockchain makes it almost impossible to be hacked and its data tampered with. Due to the nature of the blockchain and collective computing power of the network, it is extremely difficult to be successful in a cyber-attack, unlike a platform hosted on private servers.

Since blockchain provides only the authentication, we intend to provide confidentiality to the data by encrypting it with the encryption algorithm, AES [31-33] before hashing [34]. Thereby we can ensure the security of data and can make it trustworthy for users.

3.2. In Depth Review – How it works

As we mentioned in the above paragraph, the best solution is to encrypt data before creating a transaction. Once the data is encrypted, the encryption key is saved locally and sent only to the student. This makes it hard to invalidate a certificate at a later time, however we might add a piece of identifying information in the blockchain in case the serial number of the contract is lost, or we might want to develop local databases to save students ID and their associated certificate serial number.

The first node sends the signed transaction, including the transaction signature to a central server that broadcast the transaction to the blockchain network. Editing data already on the network, will have higher costs, as the entire information will have to be decrypted, edited, and then re-encrypted and re-added to the network, but this is expected to be extremely uncommon.

It is not the same for the certificate state, as changing a certificate state can be done only by the accreditation body or university, and they have the necessary permissions and ID/Serial of certificate. Another issue is the encryption key, because if the key is stolen then the students' certificate will be compromised. Despite this, a request can be made to generate a new key and re-encrypt the data; however this will be the same as editing the students' information.

As it is presented in Fig.2, the accreditation body is the first to allow universities to add and modify certificates. Although there is the possibility that any university can add certificates, but only accredited ones can add approved certificates, and at a later time it is up to the employer to take the appropriate action.

Universities are responsible for adding certificates to the blockchain, validating/invalidating them if needed, storing encryption keys and logs on a private server. Once the data has been encrypted, it is sent to a blockchain network to be stored permanently. The necessary fields needed until now are: (1) certificate serial number, (2) encrypted data and (3) certificate state. Once the university has issued a certificate, the student is provided with a QR code, which can be shown to the employer in order to check whether the certificate is valid or not.

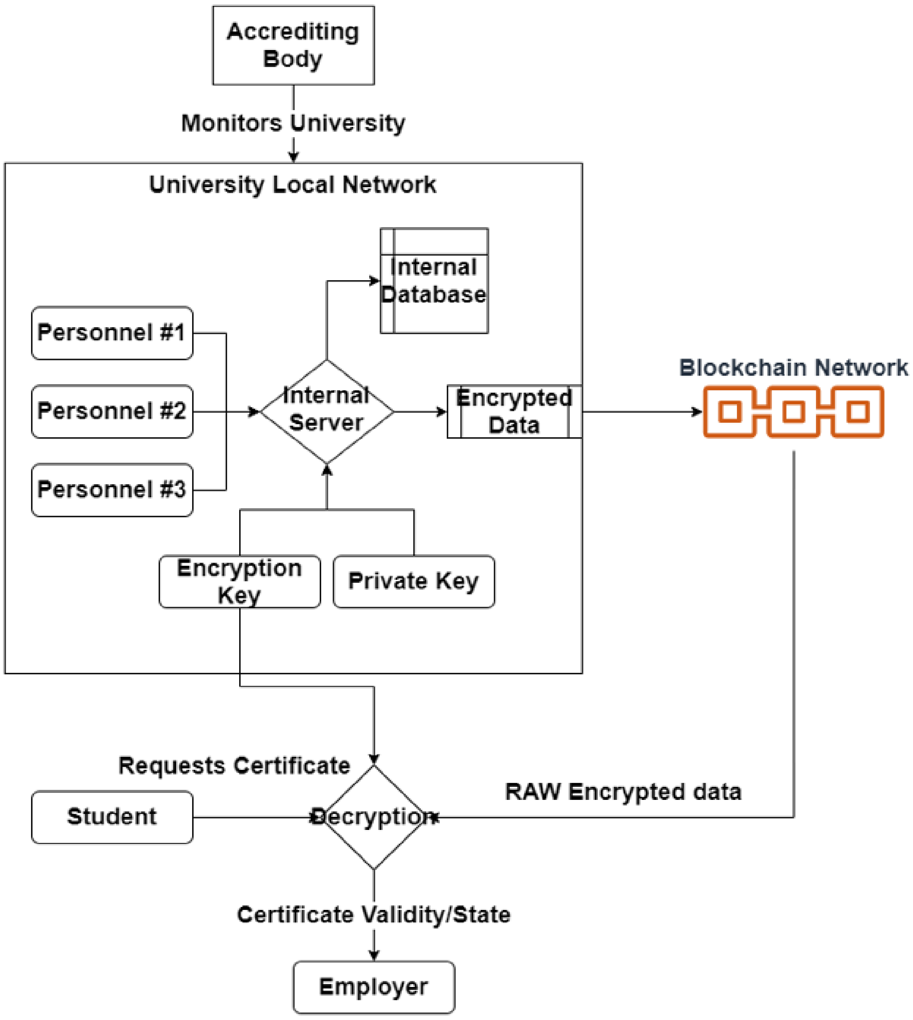


Fig. 2. In depth review of proposed solution

4. IMPLEMENTATION DESIGN AND TESTING

The development process of this application, which aims to distribute and verify academic certificates is implementing using Ethereum blockchain based smart contract. Ethereum allows the development and execution of smart contracts and “distributed autonomous applications – Dapps” [35]. Smart contracts and applications on the blockchain run on the Ethereum Virtual Machine (EVM). Operation of smart contracts on the blockchain and approval of the transactions bring costs such as: (1) amount data sent, (2) contract size in byte code and (3) transaction fees [36, 37].

4.1. Development Requirements

Since this type of application requires a blockchain network, this network incurs fees and is only used for full-developed applications. It can lead to huge financial losses in possible errors. Therefore, to deploy our solution, would be appropriate first to test it locally, and then send to the Ethereum blockchain. For development of application we need to use:

1. ***Ganache***. Ganache is part of the Truffle suite of Ethereum development tools, and it is Open-Source. It quickly creates a personal Ethereum blockchain network used to run tests commands and see how the chain operates. As Ganache comes with a GUI, and requires a separate desktop environment, we use Ganache-Cli hosted on CodeSandbox. By default CodeSandbox is an online IDE and prototyping tool aimed at developing web apps, but in this case we will use it only for ganache-cli as it enables us to quickly create an online semi-personal blockchain network.

2. ***Web3JS.*** Web3JS enables the client to communicate with the blockchain network and enable us to deploy, view, add, modify and validate contracts on blockchain network. Web3JS together with some HTML/CSS/JavaScript are used to create a simple interface to communicate with the blockchain. Additional libraries such as jQuery, Bootstrap are used to make the development easier and libraries such as Crypto-Js in order to encrypt data.

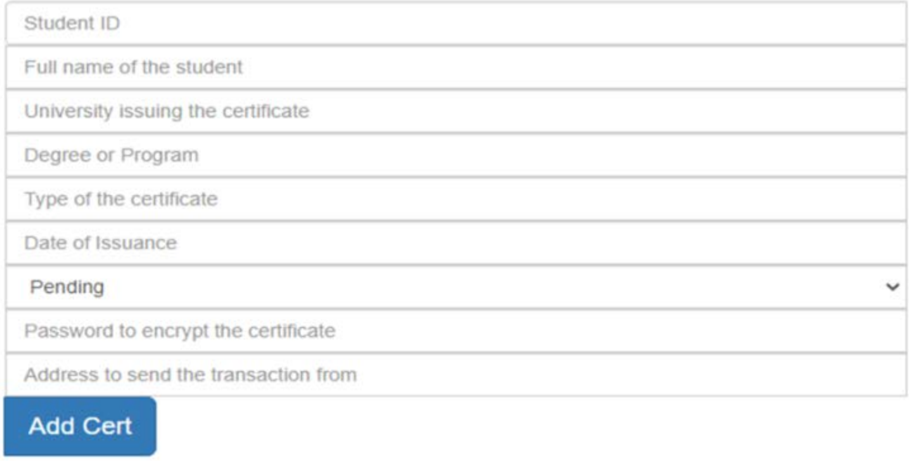
3. ***Remix.*** A Solidity word processor/IDE, Remix, is used to deploy smart contracts. It has a few extra features aside from simply writing code. After developing the smart contract, Rinkeby Ethereum Test Network is used in order to compile and test the contracts.

4.2. Interfaces

After making the appropriate installation and configuration of Ganache, we are able to deploy smart contracts on Etherem blockchain.

Once the client has started, it is presented with a screen, where there are shown 10 accounts with 100 ethers as default and private keys of each account respectively, out of which only one is unlocked. These accounts can be used to send and receive Ethereum transactions, or to make operations on smart contracts. After the user opens the interface, it is required to enter the address where the contract has been deployed.

In Fig. 3 it is presented the interface of adding certificates to the blockchain, if the contract address, that has been added before was valid. The following fields become available: Student ID, Full name of the student, issuing university, degree of program, type of the certificate, data of issuance, certificate state, encryption password and address to sign the transaction.

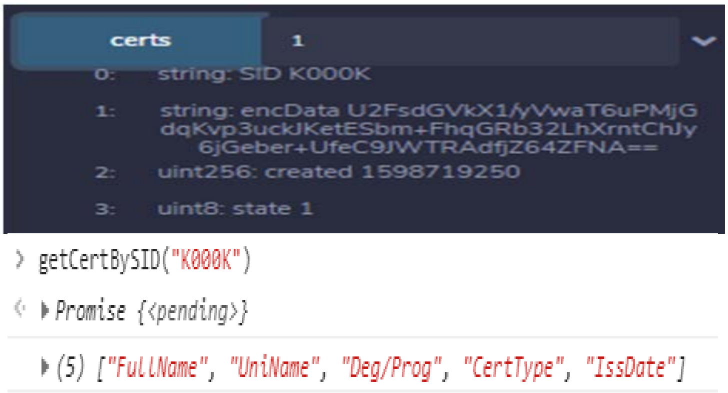


Student ID
Full name of the student
University issuing the certificate
Degree or Program
Type of the certificate
Date of Issuance
Pending
Password to encrypt the certificate
Address to send the transaction from
Add Cert

Fig.3. Interface of adding certificates to the blockchain

After the above fields have been filled, the university/personnel is required to sign the transaction using the university private key. This means that not everyone can issue certificates and not on behalf of other universities.

Once the process has been completed, the certificate is added to the blockchain after the network confirms the transaction. Even though we entered a lot of private information, the only information stored on blockchain includes: student ID, encrypted data, creation date (this is different from issuance date) and certificate state as it is shown in the Fig. 4.



```
certs    1
0:   string: SID K000K
1:   string: encData U2FsdGVkX1/yVwaT6uPMjG
     dqKvp3uckJKetESbm+FhqGRb32LhXrntChJy
     6jGeber+UfeC9JWTRAdfjZ64ZFNA==
2:   uint256: created 1598719250
3:   uint8: state 1
```

```
> getCertBySID("K000K")
<· ▸Promise {<pending>}
   ▸(5) ["FullName", "UniName", "Deg/Prog", "CertType", "IssDate"]
```

Fig.4. Deployed certificate

We have developed other functions to retrieve and decrypt the certificate based on Student ID or certificate serial number. These functions are: *getCertBySID()* and *getCertBySerial()*, which both return the following data as are presented in next section.

4.3. Contract Deploy

The Solidy code that defines how the contract behaves, is presented in Fig.5. **certCoun**t ( ) works as the certificate serial number, we can access every certificate by using its index value. Once the contract has been deployed an initial certificate is added, which has its serial number equal to 0.

```
pragma solidity >=0.4.22 <0.7.0;
contract certificate Contract {
uint public certCount = 0;
enum State {PENDING, APPROVED, DECLINED}
structcertStruct {
string SID;
stringencData;
uint256 created;
        State state;
    }
mapping(uint =>certStruct) public certs;
constructor() public {
certs[0] = certStruct("K00000000K", "Init", now,
State.PENDING);
    }
Function addCert(string memory _SID, string memory _data, State
_state) public {
for(uinti = 0; i<= certCount; i++) {
if(keccak256(bytes(certs[i].SID)) == keccak256(bytes(_SID))) {
return;
            }
}
certCount++;
certs[certCount] = certStruct(_SID, _data, now, _state);
    }
Function getCert(string memory _SID) public view returns
(string memory, string memory, uint256, State){
for(uinti = 0; i<= certCount; i++) {
if(keccak256(bytes(certs[i].SID)) == keccak256(bytes(_SID)))
{return (certs[i].SID, certs[i].encData, certs[i].created,
certs[i].state);
            }
         }
     }
}
```

Fig.5. Deployed certificate

The structure of certificate, includes *SID* for the Student ID, *encData* for the encrypted data, created for the date that signifies when the certificate has been added on the blockchain state for the state of contract pending, approved, and declined/revoked.

Costom functions include: *addCert(), getCertBySerial(), getCertById().* ***addCert()*** function takes 4 parameters: StudentID, encrypted data, state and address to sign the transaction.

getCert() function takes only one parameter which is student ID, and it returns the certificate data associated with that student Id. *getCertBySerial ()* function should be present only on the student/employer application. Once the function is called, the user is required to enter a private key linked to the address in order to sign the transaction. Various checks are made in order to make sure the fields are filled with appropriate data. Later the contract ABI, which works as an instruction set to the real contract is added and then the transaction is compiled, sent and the receipt is returned once it is available. This function returns the data from the certificate with the required serial number, and the user is required to decrypt those data using encryption key. If the encryption key is valid, the data is decrypted and shown, otherwise the operation fails. This function interacts directly with certificates on the specified index.

getCertBySID() is same as the above function, but requires StudentId instead. Unlike the previous function, this one interacts with the *getCert()* function specified in the smart contracts.

5. FURTHER DEVELOPMENT

Currently a client-side cross-platform verification application is being developed, and is halfway through. We believe that by having a fully working prototype is the only way to show the true power of the system.

For further development we will add several other features to the current smart contract, such as the ability to restrict some functions only to specific addresses (universities), and functions that enable universities to change a certificate or data.

The client side application consists of only one part. It is expected to be divided into 3 applications, one for accrediting body, one for the university and the other of student or employer. Actions such as entering an account and signing a transaction are planned to be automatic to make the process easier and logs created for each action in order to prevent abuse and add security. Application for the accrediting body and universities should be considered private and run only on a local and secure network and keep logs available for any appropriate authority to check.

The other public application should be easy to use. The proposed solution is to create a Progressive Web App (PWA) [38] which enables a web application to run on several platforms as a native application. Anyone who wants to verify a certificate should be able to scan the QR code and gets a response instantly, without having to add an encryption key manually, thus making the process more secure. This application should be easy to install on any device, iOS, Android, Windows and readily available. However each person should responsibly download/install this application form trusted sources. There is the possibility of locally saving the certificate serial number, and if this certificate is invalidated, the employer is automatically notified.

6. CONCLUSIONS

The proposed system, which is used to distribute academic certificates using blockchain adds value and increase time efficiency for issuing certificates process in education institutions and covers all the essential components of blockchain such as traceability, provenance, certification and authentication.

BCert reduces transaction and smart contract deployment costs. Smart contract transactions depend on the amount of data being added to the blockchain, however a few tests on deploying the contract and adding certificates has been conducted. The results may vary depending on the exchange rates and data being stored, but that being said, transacting approximately 170 bytes of data costs 725714 GAS, which converts to roughly $2, and the initial deployment of the smart contract costs approximately $20. We are looking into other ways to reduce the cost and increase data size, and a potential solution might introduce costs as low as $0.2 per contract, however further development and testing is needed.

BCert provides confidentiality due to using AES algorithm before creating transaction and will offer certain features such as real time online verification, third-party verification, usability and revocation.

Beyond the direct beneficiaries, issuers and users, a list of stakeholder groups includes: *(1) Ministry of education and government,* interested in better system of education, with a higher quality, part of which is also the certification process. The future of blockchain and development of actual proposed technology will give also more opportunities in the education market to have access to the best service provider that fits quality standards and gives the needed certification*; (2) Labor market, public administration (human resources offices),* will shorten the process of identification and authentication of certificates of applicants for open competition for public positions. Business and business associations will have the opportunity given by the users to how access and immediate information to see in real time the certificates; (*3) Institutions dealing with fraud cases in certifications or in education* will have more reliable data through this technology, as well as reduced number of cases in the future; *(4) Professionals* in different areas, working as freelancers, will be more secure within their market with certificates that are accessed and verified.

REFERENCES

[1] Grolleau, G., Lakhal, T. and Mzoughi, N. An introducing to the economics of fake degrees. *Journal of Economic Issues,* **3** (vol.42), 2008, pp. 673-793.

[2] Hallak, J., Poisson, M. *Corrupt schools, corrupt universities: What can be done?* Unesco Publishing, January 2007

[3] Sayed, R., H. *Potential of blockchain technology to solve fake diploma problem (Master Thesis),* University of Jyvaskyla, 2019, pp. 9-11.

[4] Zheng, Z., An overview of blockchain technology: Architecture consensus, and future trends. *Proc. of IEEE International Congress on Big Data (BigDataCongres),* Honolulu, June 2017, pp 557-564

[5] Monrat, A. A, Schelen, O., Anderson, K. Survey of blockchain from the perspectives of applications, challenges and opportunities. *IEEE Access (unpublished),* August 2019, pp. 99.

[6] Namasudra, S., Deka, Ch., G., Johri, P., Hosseinpour, M., Gandomi, A., H. The revolution of blockchain: State-of-the-Art and research challenges. *Archives of Computational Methods in Engineering,* May 2020.

[7] Leka, E., Selimi, B., Lamani, L. Systematic Literature Review of blockchain applications: Smart contracts. *Proc. of IEEE International Conference on Information Technologies (InfoTech-2019),* Bulgaria, October 2019.

[8] Carter, L., Ubacht, J. Challenges of blockchain technology adaption or E-grovernment: A systematic literature review. *19th Annual International Conference DG. '18,* Delft The Netherlands, June 2018.

[9] Mettler, M. Blockchain technology in helathare: The revolution starts here. *Proc. of. E-health networking, Applications and Services (Health.com), IEEE 18th International Conference*, Munich Germany, 2016, pp. 1-3.

[10] Christidis, K., Devetsikiotis, M. Blockchain and smart contracts for the internet of things. *IEEE Access*, Vol.4, 2016, pp. 2292-2303.

[11] Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D., Zeng, X. Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and applications. *Energies 2020,* Vol. **13**, Fabruary 2020, pp. 881-901.

[12] Ines, S., Jansen, A. Blockchain technology as infrastructure in public sector: an analytical framework. *Proc. of the 19th Annual International Conference dg.0'18*, Delft, The Netherlands, June 2018.

[13] Bellini, E., Iraqi, Y., Damiani, E. Blockchain-based distributed turst and Reputation Management System: A survey. *IEEE Access* Volume **8**, 2020, pp. 21127-21151

[14] Duan, B., Zhong, Y., Liu, D. Education application of blockchain technology: learning outcome and meta-diploma. *In parallel and Distributes Systems (ICPADS). Proc. of. IEEE 23nd International Conference*, December 2017, pp. 814-817.

[15] Alammary, A., Alhazmi, S., Gillani, S. Blockchain-based application in education: A systematic review. *Applied Sciences*, Vol. 19, June 2019, pp. 2400-2418.

[16] Nguyen, B. M., Dao, T. C., Do, B. Towards a blockchain-based certificate authentication system in Vietnam. PeerJ computer Science 6:e266, March 2020, https://doi.org/10.7717/peerj-cs.266

[17] Holotescu, C. Understanding blockchain opportunities and challenges. *Proc of. International Scientific Conference on eLearning and Software*, Bucharest, Romania, Vol.4, April 2018, pp. 275-283.

[18] Jirgensons, M., Kapenieks, J. Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability*, **1** (vol. 20) 2018, pp. 145-156.

[19] Newman, J. M. *Innovation policy for cloud computing contracts. Reasearch handbook on digital transformations*. Edward Elgar Pulishing, 2016.

[20] Gattaschi, V., Lamberti, F., Demartini, C., Pranteda, C., Santamaria, V. Blockchain and smart contracts for insurance: Is this technology mature enough? *Future Internet*, **10** (vol. 1), 2018, pp. 20.

[21] Nizamuddin, N., Salah, K., Ajmal, M., A., Arshand, J., Rehman, M.H. Decentralized document version control using EthereumBlockchain and IPFS. *Computers and Electrical Enginering Journal*, vol.76, 2019, pp. 183-197

[22] Oliver, M., Moren, J., Prieto, G., Benitez, D. Using blockchain as a tool for tracking and verification of official degrees: business model. 29th European Regional Conference of the International Telecomunications society (ITS). *Towards a Digital Future: Turning Technology into markets*, Trento, Italy August 2018.

[23] Trukanovic, M. Holbl, M., Kosic, K., Hericko, M., Kamisalic, A. EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, Vol 6, January 2018, pp. 5112-5127

[24] Gresch, J., Rodrigues, B., Scheid, E. J., Kanhere, S. S. The proposal of a blockchain-based architecture for transparent certificate handling. *1st Workshop on blockchian and Smart Contract Technologies (BSCT 2018).*

[25] Panait, A. E., Olimid, R. F., Stefancescu, A. Analysis of uPot Open, an identity management blockchain-based solution. *The 17thInterntional Conference on Trust, Privacy and Security in Digital Business*, Slovakia, June 2020.

[26] Hammed, B. Murad, K. M., Nmman, A., Ahmed, M. J. A review of blockchain based educational projects. *International Journal of Advanced Computer Sciences and Applications*, **10** (vol 10), 2019, pp. 491-499.

[27] University of Nicosia. Academic Certificates on the Blockchain. http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on-the-blockchain/

[28] Tariq, A., Haq, H. B. and Ali, S. T. Cerberus: A blockchain-based accredication degree verification system. *arXiv:192.06812v1*, December 2019.

[29] Kanan, T., Obaidat, A. T., Al-Laham, M. SmartCert Blockchain imperative for educational certificates. *Proc. of IEEE Jordan International Joint Conference on Electrial Engineering and Information Technology (JEEIT)*, Ammam, Jordan, May 2019.

[30]Omar, S., Saleh, O., Ghazali, O., Ehsan, R. M. Blockchain based framework for educational certificates verification. *Journal of critical Reviews*, **3** (vol.7), January 2020, pp. 79-84.

[31] Kamisalic, A., Turkanovic, M., Mrdovic, S., Hericko, M. Learning Technoogy for Education Challenges. *Proc. Of. 8th International Workshop, LTEC 2019*, Spain, 2019, pp. 114-124.

[32] Abdullah, A. M. Advanced Encryption Standard (AES) Algorithm to encypt and decrypt data. *Proc. of Cryptograhpy and Network Security*, June 2017.

[33] Wang, Sh., Zhang, Y. A blockchain-based framework for datasharing with fine-grained access control in decentralized storage systems”, *IEEE Access*, Vol **6**, July 2018, pp. 38437-38450.

[34] Nivethini, P., Meena, S., Krithikaa, V., Prethija, G. Data security using blockchain technology. *International Journal of Advanced and Applications (IJANA)*, Special Issue, 2019, pp. 279-282

[35] Karatas, E. Developing Ethereum blockchain-based document verification smart contract for Moodle Learning management System. *International Journal on Informatics Technologies*, **4** (vol. 11), October 2018, pp. 399-406.

[36] Buterin, V. *A next generation smart contract and decentralized application platform.* Ethereu White Paper, 2018.

[37] Kumar, D. K., Senthil, Kumar, D. S. Educational Certificate Verification System Using blockchain. *International Journal of Scientific and Technology Research*, 2020, **3** (vol. 9), pp. 82-85.

[38] Majchrzak, T. A., Biorn-Hansen, A., Gronli, T.M. Progressive Web Apps: the Definite Approach to Cross-Platform Development?. *Proc. of the 51st Hawaii International Conference on System Sciences*, 2018, pp.5735-5744

Information about the authors:

Elva Leka is Phd. Candidate Student at Faculty of Contemporary Sciences and Technologies, South East European University in North Macedonia. She works as Assistant Lecturer at Polytechnic University of Tirana, Albania. Areas of scientific research – security, blockchain implementations, distributed networks.

Besnik Selimi is Associate Professor in Faculty of Contemporary Sciences and Technologies, South East European University in North Macedonia.

Manuscript received on 09 October 2020