DECENTRALIZED ACADEMIC CERTIFICATE SYSTEM DISTRIBUTION USING BLOCKCHAIN TECHNOLOGY

Akarsh G Shroff   
Department of Computer Science and Information Systems *BITS Pilani,*Pilani, India  
f20181121@pilani.bits-pilani.ac.in

Varun Sahni  
Department of Computer Science and Information Systems *BITS Pilani,*Pilani, India  
f20200144@pilani.bits-pilani.ac.in

Under the guidance of:

Ashutosh Bhatia,

Assistant Professor, Department of Computer Science and Information Systems, *BITS Pilani,*Pilani, India

*Abstract*— *In this paper we propose to use a blockchain based system, which is employed to store, distribute and verify academic certificates so as to boost efficiency and security. It  is predicated on utilizing Ethereum smart contracts and leverages the advantages of IPFS (InterPlanetary File System), to store the certificates in an exceedingly decentralized filing 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 could also be stored on a public blockchain in a very transaction signed by private key of issuer institution which ensures the validity of documents.*

Keywords—Blockchain, IPFS, Smart Contracts, Solidity

# 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 try and do so [1-3]. Certificates which are issued in a very traditional/physical way is easily copied and their integrity and origin is tough to impossible to verify. Other issues are associated with the way these certificates are issued, delays because of administrative level incompatibilities or miscommunication, credential transfers among faculties/universities.  
Blockchain are going to be one amongst the subsequent technology revolutions thanks 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 will be applied in several domains such as: government [8], healthcare [9],  
104 International Journal on Information Technologies & Security, No 4 (vol. 12), 2020  
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 are developed for educational purposes. Blockchain Technology will transform the education industry in several 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]. during this paper we are that specialize in management of digital certificates. this process for verifying an employee candidate’s credentials are often very time- consuming, redundant and expensive, furthermore it should increase the possibilities for losing the simplest candidates to competitor companies supported the time delay. Blockchain is wont to issue unique digital assets that verify the credentials of educational degrees and certifications. this might make it much easier for potential employers to verify the degrees and save valuable time and money.  
The answer we propose during this paper, uses concept of Blockchain and smart contracts to distribute and verify certificates. Blockchain areoften implemented as: (1) decentralized network, in sense that there's no node that acts because the central server for the network, (2) distributed network, in sense that responsibilities are shared by the nodes. For the project’s implementation we have employed Ethereum Platform network [19] and Solidity language [20] so as to deploy smart contracts. Certificates are going to be saved 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 to blame 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 will be used as a singular 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 novel identifier/serial number that's 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 personal key, which is merely available to the university and therefore the issuing authority. On the opposite hand, the accreditation body uses its private key so as to accredit the university similarly. When the university issues a certificate, it's automatically marked as valid/accredited and put into the network.

# Proposed solution

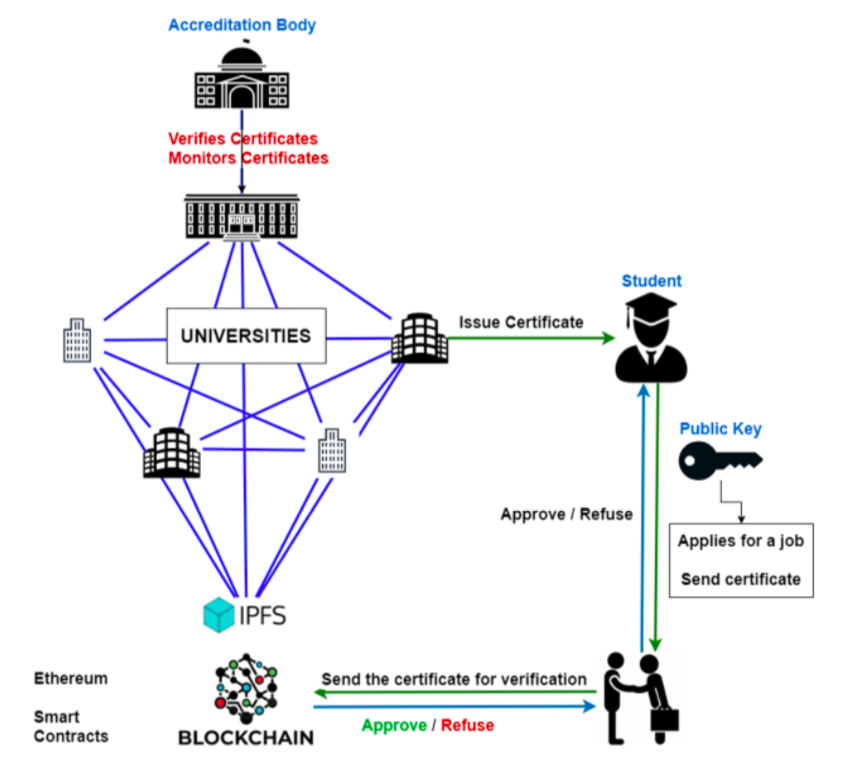
## Solution

In this study, it's aimed to verify and distribute digital certificates given to the students, by using Ethereum Blockchain based smart contract. artificial language that's wont to deploy smart contracts is termed “Solidity”. We have chosen Solidity, because it's a well-established programing language used for coding smart contracts; other alternatives don't 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 wise Contract.  
The main roles proposed for the system are: (1) issuer, which may be universities or training centers; (2) users, which might be students, employers or academic institutions; (3) Accreditation body, which serves to validate the certificate. Uploading certificate to the blockchain is finished only by issuers, who can: add credentials, view their credentials or issue credentials to user. On the opposite 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 not be removed, and each activity regarding this contract is publicly available. counting on how universities and accreditation bodies work together, a certificate may be verified at a later time, or upon its insertion into the blockchain.

## Architecture of the System

Authenticity of a certificate is easily validated and tracked back to the issuing and accreditation body;  
International Journal on Information Technologies & Security, No 4 (vol. 12), 2020 107  
otherwise, the certificate is marked as invalid, although it'll 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 previous 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 relies on how the system are implemented.

Having this platform rely upon blockchain makes it almost impossible to be hacked and its data tampered with. Thanks to the character of the blockchain and collective computing power of the network, it's extremely difficult to achieve success in a cyber-attack, unlike a platform hosted on private servers.



# 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 event 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].

## Development Requirements

Since this sort of application requires a blockchain network, this network incurs fees and is just used for full-developed applications. It can cause huge financial losses in possible errors. Therefore, to deploy our solution, would be appropriate first to check it locally, so send to the Ethereum blockchain. For development of application we'd like to use:

* **Ganache.** Ganache is a component of the Truffle suite of Ethereum development tools, and it's Open-Source. It quickly creates a private Ethereum blockchain network wont 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 internet IDE and prototyping tool geared toward developing web apps, but during this case we are going to use it just for ganache-cli because it enables us to quickly create a web semi-personal blockchain network.
* **Web3JS.** Web3JS enables the client to speak with the blockchain network and enable us to deploy, view, add, modify and validate contracts on blockchain network. Web3JS along with some HTML/CSS/JavaScript are wont to create an easy interface to speak with the blockchain.

Bottom of Form

## Further Development

For further development we'll add several other features to this smart contract, like the flexibility to limit some functions only to specific addresses (universities), and functions that enable universities to vary a certificate or data.  
The client side application consists of just one part. it's expected to be divided into 3 applications, one for accrediting body, one for the university and also the other of student or employer. Actions like entering an account and signing a transaction are planned to be automatic to create the method easier and logs created for every action so as to forestall abuse and add security. Application for the accrediting body and universities should be considered private and run only on a neighborhood and secure network and keep logs available for any appropriate authority to test.

# conclusions

The proposed system, which is employed 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 like traceability, provenance, certification and authentication.  
BCert reduces transaction and smart contract deployment costs. Smart contract transactions rely on the quantity of knowledge being added to the blockchain, however some tests on deploying the contract and adding certificates has been conducted. The results may vary betting on the exchange rates and data being stored, but that being said, transacting approximately 170 bytes of knowledge costs 725714 GAS, which converts to roughly $2, and also the initial deployment of the smart contract costs approximately $20. We are looking into other ways to cut back the value and increase data size, and a possible solution might introduce costs as low as $0.2 per contract, however further development and testing is required.  
  
Beyond the direct beneficiaries, issuers and users, an inventory of stakeholder groups includes: (1) Ministry of education and government, curious about better system of education, with the next quality, a part of which is additionally the certification process. the long run of blockchain and development of actual proposed technology will give also more opportunities within the education market to possess access to the most effective service provider that matches quality standards and provides the needed certification; (2) market, public administration (human resources offices), will shorten the method of identification and authentication of certificates of applicants for open competition for public positions. Business and business associations will have the chance given by the users to how access and immediate information to work out in real time the certificates; (3) Institutions coping with fraud cases in certifications or in education will have more reliable data through this technology, moreover as reduced number of cases within the future; (4) Professionals in several areas, working as freelancers, are safer within their market with certificates that are accessed and verified.

##### References

1. [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. [2] Hallak, J., Poisson, M. *Corrupt schools, corrupt universities: What can be done?* Unesco Publishing, January 2007
3. [3] Sayed, R., H. Potential of blockchain technology to solve fake diploma problem (Master Thesis), University of Jyvaskyla, 2019, pp. 9-11.
4. [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. [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. [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. [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. [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. [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. [10] Christidis, K., Devetsikiotis, M. Blockchain and smart contracts for the internet of things. *IEEE Access*, Vol.4, 2016, pp. 2292-2303.
11. [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. [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. [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. [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. [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. [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. [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. [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. [19] Newman, J. M. Innovation policy for cloud computing contracts. Reasearch handbook on digital transformations. Edward Elgar Pulishing, 2016.
20. [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. [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. [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. [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. [24] Gresch, J., Rodrigues, B., Scheid, E. J., Kanhere, S. S. The*st*proposal of a blockchain-based architecture for transparent certificate handling. *1 Workshop on blockchian and Smart Contract Technologies (BSCT 2018).*
25. [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. [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. [27] University of Nicosia. Academic Certificates on the Blockchain. http://digitalcurrency.unic.ac.cy/free-introductory-mooc/academic-certificates-on- the-blockchain/
28. [28] Tariq, A., Haq, H. B. and Ali, S. T. Cerberus: A blockchain-based accredication degree verification system. *arXiv:192.06812v1*, December 2019.
29. [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. [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. [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. [32] Abdullah, A. M. Advanced Encryption Standard (AES) Algorithm to encypt and decrypt data. *Proc. of Cryptograhpy and Network Security,* June 2017.
33. [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. [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. [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. [36] Buterin, V. A next generation smart contract and decentralized application platform. Ethereu White Paper, 2018.
37. [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. [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