Advances In Multidisciplinary & Scientific Research
A Multidisciplinary & Interdisciplinary Journal
Volume 8, No 2, June 2022 Series

A Validated Smart Contract Model For Certificate Verification System.

[1]Alu, E.S., [2]Murphy, B.B & [3] Yunana, K.
[1]Department of Computer Science, Nasarawa State University, Keffi, Nigeria
[2]Department of Computer Science, Niger Delta University, Bayelsa State, Nigeria.
[3]Department of Computer Science, Nasarawa State University, Keffi, Nigeria
E-mails: estheralu@nsuk.edu.ng; tukamurphy@ndu.edu.ng, kefasyunana@nsuk.edu.ng
Phone: +2348035995804; +2347034433507, +2348061560912

ABSTRACT

As technology is advancing, the society is experiencing advancement most especially in academic certification. Globally, over 30 million students' graduates yearly acquiring different academic certificates from a college after completing an undergraduate or postgraduate programs, or transcripts during their entire period of studies. In the same vein, the students are required to produce their certificates in institutions or companies either for admission or job pursuit. Acquiring certificates is not a problem but tracking these certificates and validating their authenticity manually becomes complicated and tedious to do. Most institutions and organizations verify certificates by using a third party which can be bribed to authenticate a forged certificate as being valid. This poses adverse negative effects like admitting the wrong students or employing an amateur for a position in an organization. Although, several researches have been carried out in authenticating the integrity of certificates presented by the user but to make the data more secure and safe, everything needs to be digitalized with the principle of Confidentiality, Reliability, and Availability by employing the distributed ledger technology (Blockchain). Smart contracts are developed on the blockchain platform to implement a model for authenticating and verifying academic degrees. However, the deployed smart contract may be vulnerable to hackers and this could result in huge financial loss and inefficient functional system. In this paper, we proposed the validation of smart contract codes for implementing educational certificate platform for security vulnerability and optimal performance.

Keywords: Blockchain Technology, Smart Contract, Validation, Certificate Verification, Vulnerabilities.

Aims Research Journal Reference Format:
Alu, E.S., Murphy, B.B & Yunana, K. (2022): A Validated Smart Contract Model For Certificate Verification System. Advances in Multidisciplinary and Scientific Research. Vol. 8. No. 2, Pp 1–10. www.isteams.net/aimsjournal
DOI: dx.doi.org/10.22624/AIMS/V8N2P1

1. INTRODUCTION

Blockchain is an emerging technology that is capable of shaping everyday life by disrupting traditional products and services due to its decentralized nature and ability to run smart contracts. It exists to tackle issues such as lack of trust, non-repudiation, and the high cost of transaction execution, security and reliability of a partner in exchange [3].

As a result, the innovative technology will help to handle the emerging issues in existing certificate issuance and verification system. Certificate verification is a process whereby degree certificates issued by colleges are verified to determine its authenticity and reliability [5]. Currently in Universities, degrees are issued in paper form to the students at the conclusion of his/her academic programs. Consequently, so many academic scholars are involved in forging degrees and credentials. Besides the offline collection of fake academic degrees, many on-sites issue fake degrees and certificates. They exploit the system's inability to check the authenticity and validity of college degrees. However, individuals who are indulged in such illicit act of forging academic certificates perform badly in business and could be involved in fraudulent activities for self-gain. Due to diversification and decentralization in education, the need to maintain reputation, trust in certification and evidence of learning arises. Everyone has to reveal his/her certificate to any institution for admissions into colleges and organizations for jobs application.

Conventionally, a third party which cannot validate the originality of the certificate is hired. Also, once lost or damaged, re-application becomes complex and consumes a lot of time [5] for academic institutions to re-issue the misplaced certificates. Alternatively, digital certificate is easier, paper-saving but time consuming. However, to handle the surge of fake degrees in education, blockchain emerge as an enabling technology to ease the issuance and verification of academic degrees and certificates presented by users for diverse purposes. Inappropriate deployment of the developed smart contract can lead to financial loss (DAO Attack 2016) and loopholes which the attacker can use to initiate an attack on the contract. Our study proposed a validated smart contract system for online certificate verification. Besides authenticating and verifying academic certificates, this study will help to ensure that the deployed smart contract codes is validated for functional objectives and optimized performance. The proposed system will remove loopholes in our present system and also yield a concrete and effective solution.

2. PREVIOUS RESEARCH

A few studies have been conducted on utilizing blockchain technology for certificate authentication. Grech and Camilleri [1] presented a report on the fundamental principles and potentials of the distributed technology in the educational sector. The authors further explained how the distributed technology can affect institutional norms and empower learners. In addition, the study proposed eight scenarios in which the technology can be applied in education. In another work, Lamkoti et al [4] proposed a model for verifying an academic certificate and generating transcript using the blockchain. The authors demonstrated the need for a platform for tracking academic certificate and validating the authenticity. The hash code of the generated certificate is recorded on the blockchain while the original document is stored in the IPFS (Interplanetary File System). The authors were able to design a system which will automatically generate and validate certificate. Similarly, Yao et al. [6] developed a model for resolving the problems in authenticating an educational certificate. The proposed model centered on the need for adequate data security. However, the authors' ultimate goal was to develop a framework, by inspiring an open PDS framework for autonomous deployment of PDS. Some research studies demonstrated the use of blockchain programs such as smart contract for verifying digital certificates.

For instance, Cheng et al. and Zhao et al. [7] [8] developed decentralized programs for online certificate. However, the program was able to handle the issue of certificates counterfeiting, and verifying electronic certificates using the innovative technology but could not create a related QR code and inquisition string code to the paper certificate. In another paper, Xie et al. [9] conducted a research on utilizing an Ethereum Virtual Machine (EVM) for decentralized smart contract certificate system. In the proposed model, the difficulties in preserving and managing traditional paper testimonials, poor reliability and preventing fraud was sorted out. The study also focused on resolving the problem of authenticating and verifying certificate and provided a reliable and trustworthy blockchain-based e-certificates. Besides the development of smart contracts for a certificate system, Ahubele and Ndukwe [10] proposed a verified smart contract model on Ethereum blockchain to detect counterfeit certificate. The study focused on saving the society from the effect of certificate forgery by providing a verified model against smart contract security vulnerability and certificate forgery.

3. OVERVIEW OF DISTRIBUTED LEDGER TECHNOLOGY

The Distributed Ledger Technologies (Blockchain) paved way for parties to exchange digital transaction without the need to trust one another or involve a trusted third party [13]. The distributed ledger is used as a store of value such as money and land titles and a record of data which include medical records and digital certificates. On a simplified level, DLTs represent a category of databases that are provided for storing, recording, sharing and synchronizing data among a wide range of computers and network participants. These systems of databases can work easily and safely without the requirement of any focal gathering or focal overseer that each member knows and trust. DLT tasks are planned so that information recorded and conveyed through the systems has an elevated level of trust value, and each member in the system is allowed access to that information.

Initially, DLT was used for financial services, but with time, the use of DLT extended to e-voting, Health sector, an Insurance sector, Internet-of-Things (IoT), Organization Supply chain, etc. Blockchain is an aspect of the distributed ledger technology (DLT) which is currently gaining attraction in existing literature especially from a cryptographic point of view. As a field in distributed ledger technology, different researchers from diverse perspectives have described the ledger as a trust layer, which combines the peer-to-peer networks (P2P), cryptography and hash technology to eradicate the service of a sole administrator or control [14]. DLTs are not all blockchain, since blockchain utilizes cryptography in recording and synchronizing data into a chain of existing blocks [13]. Once an update is done on the database, it is guided by the underlying principles and are shared amongst the participating members [15].

4. SMART CONTRACTS

Today, blockchain-based smart contracts are utilized in in a variety of transaction use cases and applications ranging from IoT and Finance to Supply chain and creative art gallery. As a major feature in blockchain technology, smart contracts are set to execute pre-determined conditions based on "if/then" condition [11]. These computer codes contain rules enforced by contractual parties in such a way that once they are coded and entered into the blockchain, the contract cannot be changed but operates in accordance with its programmed instructions [12].

However, a smart contract is described as a set of distributed agreements involving functions and data that are automatically executed when terms are met. Additionally, it is an Ethereum Account that runs on an Ethereum blockchain. An Ethereum Account is made up of ether (ETH) as a balance that enable users' to communicate with a smart contract. The transaction executes a predefined-function on the smart contract code and enable users' access to the smart contract data. In 1996, Nick Szabo, a computer scientist, lawyer and cryptographer first coin the term "Smart Contract".

Szabo mentioned that the "smart" in a smart contract explained the enhanced functionality than the native paper-based method. Furthermore, Szabo description of smart contract pictured it as a *digital vending machine that must be* executed whenever a person puts money in the machine and gets the product in return. For instance, to get a drink from a vending machine, thus: money versus drink selection = dispensed drink. Smart contracts are created using solidity and Viper programming Languages and deployed over a blockchain network for execution. Ether (Ethereum crypto-currency) is needed for the deployment process.

Developers classify smart contracts for developing applications into four categories, namely:

a) **DAO (Decentralized Autonomous Organization)** – describes established and enforced rules by members of the organization which cannot be influenced by external entities irrespective of their stake.
b) **Automated Contracts** – consists of smart contracts that are legally enforced.
c) **Applied Logic Contracts (ALCs)** – these are contracts that exists in a distributed network with the user's front-end interface.
d) **Decentralized Applications** (DApps).

5. SMART CONTRACT SECURITY AND VULNERABILITY

Several occurrences have revealed vulnerabilities that have occurred in smart contract development in time pasts. In 2017, about $150m worth of Ether was stolen from parity organization due to critical vulnerability seen in their Ethereum smart contract. Also In 2016, over $50m worth of ethers was stolen by hackers as they exploit the Decentralized Autonomous Organization (DAO) named Genesis, due to security loophole in the system. Similarly, in August 2021, Poly Network, which was one of the biggest crypto-currency heists was attacked and over $600m worth of crypto currency was stolen. The hackers exploited a vulnerability in the digital contracts to launch the attack. Implementation of smart contract is visible for all users as a result of the transparency feature of blockchain. However, security loopholes and vulnerabilities can be exploited by hackers or cybercriminals to cause damage in an organization's smart contract and revenue loss.

Therefore, to prevent such situations, it is better to have a clear understanding of smart contract implementation, security functions and securing a blockchain-based-contract against hacking and cyber-attacks. Smart contract security must be initiated before developing the source codes i.e. during planning, design, and development processes and finally by providing security measures against cyber-attacks and potential vulnerabilities such as re-entrancy, front running, ETH send a rejection, integer overflow/underflow, Denial-of-Service, etc. Validating the smart contracts is necessary to ensure that the system is designed according to specification and functional goal.

6. SMART CONTRACT PRACTICES IN MITIGATING VULNERABILITIES

i. Secure Coding Best Practices

Various programming languages such as Solidity, Java, Vyper and GO are available for developing the smart contracts for deployment on the blockchain. The best coding practices for the design, implementation, and deployment of smart contracts are highlighted below:

a) Give a detailed specification of the smart contracts in clear and plain English.
b) Slither printer can be utilized in generating schema and architectural diagrams.
c) For solidity programming language, code documentation is done using Natspec format.
d) Some codes should be kept off-chain.
e) Migration or upgrading procedures are documented before the deployment.
f) Compose functions by writing small and meaningful functions, while splitting the logic through multiple contracts or grouping similar functions.
g) The inheritance tree must be as short as possible using Slither's inheritance printer.
h) Events loggings and operations implementation.
i) Be cautious of the warning section stated in Solidity's documentation.
j) Utilize libraries that are adequately tested.
k) Use Slither, Echidna, and Manticore to write customer checks and properties.
l) The programming language compiler must be utilized.
m) Smart contracts must be monitored regularly after deployment.
n) Enhanced security for the smart contracts wallets using cryptography.
o) An incidence report plan must be designed due to the vulnerability of the ethereum-based smart contract.

ii. Smart Contract Security Audit and Pen-testing

Hackers can exploit potential loopholes and vulnerability despite building a secure and bug-free smart contract. The entire platform as well as the smart contract can be compromised and millions of digital currency stolen. Pen-testing and security audit must be done periodically for a smart contract to resolve this problem. Security audits and pen testing exposes any vulnerabilities and fixes observable weaknesses before a hacker tries to launch an attack.

The steps for smart contract audit and pen-testing are as follows:

a. Vulnerable code and inconsistency can be identified using static analysis of contract code.
b. smart contract codes security analysis is performed using tools like Mythril, MythX, Echidna, Oyente, Manticore, ERC20 verifier.
c. The SWC Registry must be tested for vulnerabilities.
d. A bug bounty program during testing phase is carried out using Rinkedby.io or Kovan testnet.
e. Identified vulnerabilities in the system must be reported and recommendations must be specified for fixing those vulnerabilities.
f. Both internal security team and external security auditors are required for conducting a security audit or pen-testing for organization's smart contract.

iii. Blockchain Security Checklist
A checklist for the security of smart contract blockchain must be followed.

iv. Automated Vulnerability Scanners
An automated security vulnerability scanner will help to identify bugs in the contract source code, which can lead to security vulnerabilities and initiate a variety of attacks. For example, Securify (open-source security scanner for Ethereum smart contract)is used for security vulnerability detection.

v. Smart Contracts Audit Tools
The available smart contract audit tools are SWC-registry for smart contract weakness and vulnerabilities; MythX for Smart contract security analysis API; Echidna for fuzzing/property-based testing of Ethereum smarts contracts; Manticore for contract symbolic execution; Oyente for static analysis; SmartCheck for Security analyzer, Octopus for smart contract security analysis framework and awesome Buggy ERC20 Tokens.

7. METHODOLOGY
In this section, we presented the system methodology. This is divided into three segments: system design, verification and validation process; thus:

A. System Design
In this study, a certificate system was proposed using the distributed ledger technology. The system's application was programmed to run on EVM (Ethereum Platform). In the system, three classes of users (college, students, company) were analyzed. Colleges or certificate issuing authority grant certificates to students after completion of course study according to the university requirements, the students can access the certificate portal to request for the e-certificate and browse the system database for lists of published students issued certificates after meeting the university requirements. Users' access is reviewed and approved if coditions for issuing the certificates are met.

After the students have received the certificates applied for, they submit the hash of the certificate which links the students with his certificate to the company for validation, authentication and determine whether the certificate is genuine before granting the students the job opportunity applied for. The original document is stored in the Interplanetary file while the hash of the certificate will be stored in the blockchain. The proposed system provides an easy means to verify and authenticate certificate. The study also carried out validation of smart contract in order to ensure that functional goals are met.

The system is composed of modules such as:

i. Blockchain: Is a transparent and immutable database where records are validated and kept.
ii. Ethereum (EVM): Is a decentralized platform where smart contracts are deployed. Ethereum is a second generation blockchain mainly for developing smart contracts.
iii. Solidity: Is a JavaScript like language mainly for developing smart contract on various blockchain platforms.
iv. MetaMask: It is a web wallet which interface with Remix integrated Development Environment for building smart contract. MetaMask is both a wallet and a development environment that enable the successful execution of decentralized applications.

v. Robsten: Is an Ethereum test network used by developers to test their codes and perform some actions.
vi. Truffle: Truffle makes compilation, linking and binary management of smart contracts in solidity language.
vii. IPFS: Is an Interplanetary file system, a peer-to-peer network for recording, saving and sharing information in a distributed file.

B. Verification Process

Blockchain is a decentralized and distributed ledger where transactions are recorded in different blocks. These blocks are linked together by cryptographic hash and hashing algorithm. In this study, the college grants certificate to students and record the student's data into the college data base file. Next, the system will automatically record the hash number of the student on a blockchain, where the certificate system verifies all the data. Instead of the normal procedure of sending certificates hard copies, colleges will grant electronic certificates containing a quick response code or hash code to students once their data have been verified successfully. The graduate gets the electronic file of the digital certificate and the hash number. In applying for a job, the graduate simply sends the serial number or electronic certificate with a quick hash code to the target companies. The companies will then send users' information to the system for verification, the system determines if the serial numbers are legit or not.

C. Validation Process

The deployed smart contract must be validated for optimal performance during deployment and auditing on Etherscan explorer. The performance of any smart contract is determined by the code quality. Consequently, smart contracts audit must include performance validation in order to reduce the cost of poorly optimized contracts during execution. In this study, we proposed smart contract validation which include checking the code for any errors that might slow down or affect other aspects of the contract's performance in some way. Initially, a performance review is done by formal verification to see if the contract executes in accordance with the contractual agreement reached by both parties. Blockchain technology provides a platform for reducing certificate forgery by building applications for verifying academic degrees and ensuring that the deployed contracts meet design requirement by validation.

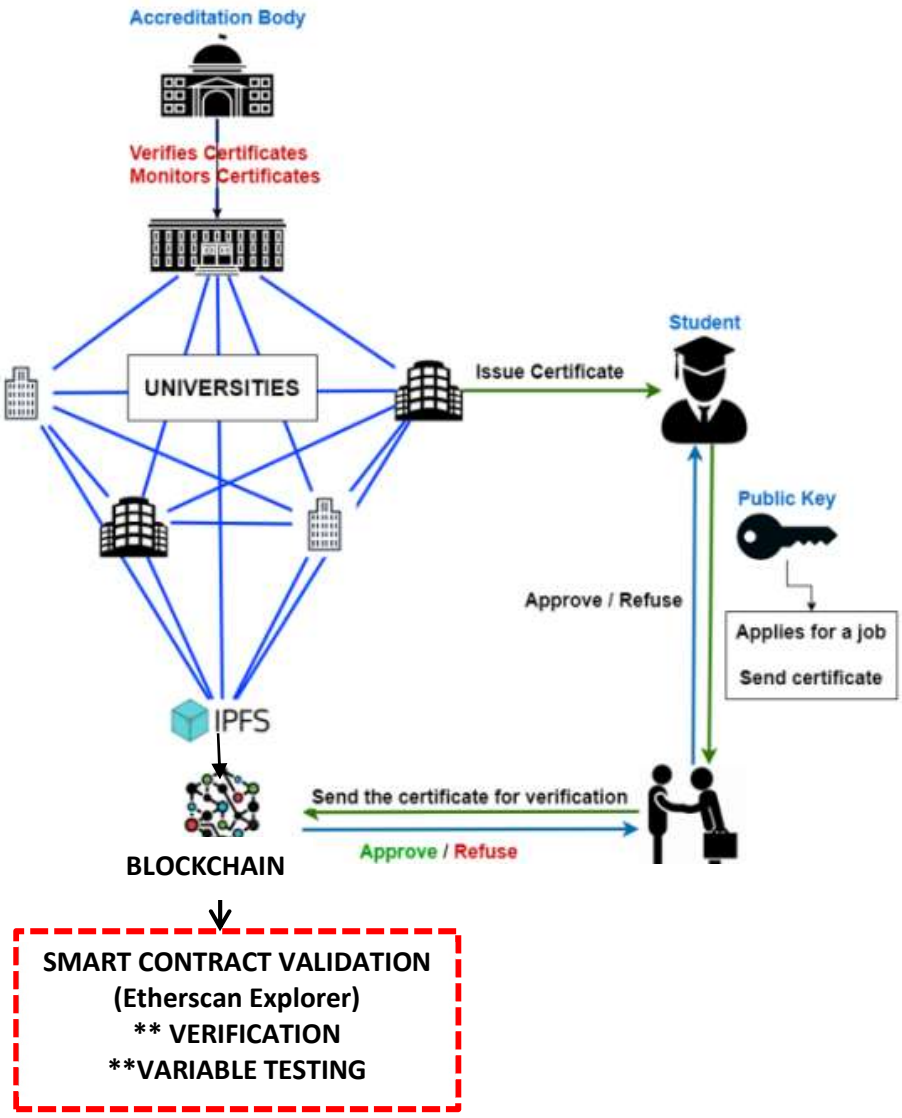

Figure 1: The Proposed System Architecture.

10. CONCLUSION AND FURTHER RESEARCH

Most universities uses QR Codes which are online track and trace method to check the legitimacy of degrees when the QR Codes are scanned. Although the use of blockchain technology in education are more beneficial but the research in blockchain for education is still at infancy. With immutable feature, blockchain helps to achieve a system where all processes are transparent and changeable.

Our proposed system will help to automate the generation of e-certificate, reduce the tedious method of verifying academic certificate and ensure that the smart contract is verified and validated against loopholes and vulnerabilities. Our proposed model will be much more reliable as it does not need the intervention of any third party. In the future, we recommend a real life implementation of the model using any institution as a case study.

REFERENCES

1. Grech, A and A.F Camilleri. Blockchain in Education. 2017. JRC Science for Policy Report. 1-136.
2. Grupta, M. Blockchain for Dummies;IBM Limited Edition. https:www-01.Ibm.com/common/ssi/cqui-bin/ssialias?html fid=XIM12345UstN&/
3. Kumutha, K and Dr. S. Jayalakshmi. Blockchain Technology and Academic Certificate Authenticity-Review . Conference Paper.
4. Lamkoti, R.S., D. Maji and H. Shetty. Certificate Verification System using Blockchain and Generation of Transcript. 2021. *International Journal of Engineering Research and Technology (IJERT).* 10(3). 539-544.
5. Billah, S., N. F. Hossan, R. Pollobe, N.M. Abir, A.Z. Zarin and Dr. M.F. Mirdha. Blockchain based Architecture for Certificate Authentication. 1-10. https://ssrn.com/abstract=3842788.
6. S. Yao, J. Chen, K. He, R. Du, T. Zhu and X. Chen. PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management. 2019. In IEEE Access.7. 6117- 6128. Doi: 10.1109/ACCESS.2018.2889898.
7. J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.
8. J. Zhao, Z. Lin, X. Huang, Y. Zhang and S. Xiang, "TrustCA: Achieving Certificate Transparency Through Smart Contract in Blockchain Platforms," 2020 International Conference on High Performance Big Data and Intelligent Systems (HPBD&IS), Shenzhen, China. 1-6,doi:10.1109/HPBDIS49115.2020.913058.
9. R.Xie et al., "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System," in IEEE Internet of Things Magazine. 3(2). 44-50. June 2020, doi:0.1109/IOTM.0001.1900094.
10. Ahubele, B.O. and Ndukwe, O.E. A Verified Ethereum-Based Smart Contract Model To Detect Counterfeit Educational Certificate. Journal of Advances in Mathematical and Computational Sciences.
11. Mearian, L. (2019).What's a smart contract (and how does it work)? Retrieved 20/11/2020. https://www.computerworld.com/article/3412140/whats-a-smart-contract-and-how-does-it-work.html
12. Delmolino, K., M. Arnett, A. Kosba, A. Miller and S. Elaines (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. *International Conference on Financial Cryptography and Data Security.*79-94. Retrieved 15/10/2018. https://etherscan.io/contractsVerified .

13. European Commission. (2019). Blockchain Now and Tomorrow. In European Commission. Science for Policy report by the Joint Research Centre (JRC). https://doi.org/10.2760/29919
14. Mercy Corps (2017). A Revolution In Trust: Distributed Ledger Technology in relief and Development. *https://www.mercycorps.org/sites/default/files/*