International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9, Issue-7, May 2020

Blockchain based Certificate Issuing System using Smart Contracts

Meerja vali Shaik, Ch. Rupa, M N S Koundinya, Rohith Gadde, Harish Donepudi

Abstract: ***Nowadays everything seems to be original and it's being herculean task to identify which is not real. It may be a currency for people or valued currency for students such as certificates. A lot of fraudulent parties have made money by encouraging the duplicate certificates in society. As a result, low talented or inefficient people are getting more and they are being responsible for the degradation of any nation's value. A blockchain-based certificate is a prime solution for the above problem. In this work, would like to discuss the functioning of a smart contract in favor of Issuing, verifying, and revoking the certificates through gas value[9] deductions. Thus our certificate can provide the added assurances of evidence of origin in a transparent manner using.***

Keywords : Blockchain, Smart contracts, Certificates, Gas value, Transparency.

I. INTRODUCTION

A. System overview

Advancement in technology is helpful for mankind in many ways such as saving our time, ease of communication, improved banking sector, better hospitality, and fast mobility of every field. To add advancement in the education certificate issuing system my project is built to counterfeit the fraudulent practices occurred in the issue of academic certification thorough using disruptive technology like block-chain. Usage of paper based documents, centralized database repositories for generating certificates is less secure, not more reliable, and inefficient. Because of all these sometimes loss of records happening, fake certificates birth rate increasing. No other security system challenges as 100 percent secure system other than the blockchain-based system nowadays. Using blockchain[3] as the main theme we proposed a certificate issuing system that works securely.

Revised Manuscript Received on May 30, 2020.
***** Correspondence Author
Meerja vali Shaik*, Department of Computer Science and Engineering, VR Siddhartha Engineering College, Vijayawada, Kanuru. Email: meerjavali98@gmail.com.
Ch. Rupa, Professor, Department of Computer Science and Engineering, VR Siddhartha Engineering College, Vijayawada, Kanuru. Email: yaswanth95263@gmail.com
Rohith Gadde, Department of Computer Science and Engineering, VR Siddhartha Engineering College, Vijayawada, Kanuru. Email: rohithgadde4@gmail.com
M N S Koundinya, Department of Computer Science and Engineering, VR Siddhartha Engineering College, Vijayawada, Kanuru. Email: suryamanikonda@gmail.com
Harish Donepudi, Department of Computer Science and Engineering, VR Siddhartha Engineering College, Vijayawada, Kanuru. Email: harishdonepudi@gmail.com

Our system runs on the smart contract using Ethereum-solidity [1] environments or using a truffle suite that can manage our smart contract for custom deployments. We should extend plugin like metamask[11] because it acts as a gateway for application.

B. Motivation

Immense use cases for the educational systems, corporate companies, and other sectors that use qualified, graduated students as their workforce enhanced or resolved by this disruptive technology named blockchain[3,4]. A student's professional growth is validated by certificates he/she owned. Duplicate/fake certificates are generated because the records are offline and there is no superior authority to cross-check or to validate. Only power resided to single man/authority they can manipulate for malpractices, for any other benefits. Many block-chain applications failed due to lack of awareness about this technology. All the systems are resting in books because of the unknown facts of block-chain.

C. Objectives

Putting an end to existing technologies based on the stamp and seal procedure for certificate generation on paper. Developing an open standard that can create or issue, revoke and verify academic certificates without the use of paper. Creating a source that we can share our certificates and verify from anywhere and anytime.

II. RELATED WORK

T. Kannan, et. al [1] designed a system as per the current demand of academic certificates is more because it's an identity. Applications of passport, visa, driving license, and many other require standards like academic certificates. To obtain these benefits from academic certificates some people making actions like forging documents, photography edits, and deceiving system. Hence Al- Zaytoonah University of Jordan decided to develop an authentic system that checks the authenticity of the document/certificate using block-chain technology. Therefore they developed a smart contract and named it as smartcert[1] and implemented it in Ethereum platform located at remix.ethereum.org. They make use of database for storing all the certificates in a single room. A. Badr, et.al [2] discussed about a permission blockchain system to verify academic records. Nowadays everything is automated they save or time but coming to education system still they are using manual process for certificate/transcripts transfer. Making this into an automatic a permissioned block-chain based system developed which doesn't require proof of work for validation as it named permissioned.

Using Hyper ledger[2] fabric system developed with sendTranscript() function transfer of certificates/transcript happens. Ownership of the transcript is resided to only one person. Transcript transfer happens based on set of rules written in the hyperledger, owner.

J. Cheng, et. al [3] proposed a system for digital certificates using blockchain technology because millions of people graduate each year. Graduated people continue their education or go to the workplace. Wherever they go whatever they choose their professional growth is measured by their academic certificates, diplomas they pursued. But academic certificate contains only two inputs such as certifier name (college/school), student name, therefore some third parties making advantage of this and forging academic certificates for many purposes like money, power, and to dishonor the reputation of the system. Thus they developed an anti-forge[3] mechanism for the education system, other systems that consider academic certificate for validating the professional growth of the students/employees joining their institution/company. This anti-forge[3] mechanism completely built as blockchain-based application thus record each transaction of a certificate issued by the authority and creates a block for a group of transactions. Each transaction is recorded with timestamp values.

A. Srivastava, et.al [5] proposed a framework Companies, universities, and many other private sectors face difficulties in background verification. Lot of man power and time required for background verification even though not getting cent percentage successful results. To overcome thissystem developed that can issue certificate on blockchain and makes easy for verification through online platform. System works on consensus which uses a multi signature protocol for issuing certificate. Every node in the system obeys the consensus[5] hence all the transactions are recorded and framed in a ledger, If any new node like X a stakeholder comes verify the certificate he joins the blockchain network therefore he gets access to the public ledger and verifies.

III. METHODOLOGY

A standard system which is more secure, more reliable that can create or issue, revoke, and verify academic certificates, and harder to forge academic certificates. In our System, the two important actors are one is institution authority and the second actor is student/others. The first actor performs all the three actions such as issuing, verifying, and revoking certificate but the second actor can only perform one verify action as shown in the Fig.1 Block diagram. Each action performed by the institution authority converts into a transaction. One or group of transactions forms a block. Whenever a new block is created it will automatically be linked to the previous block in the network. Therefore a chain of blocks came into existence while the system works on and conclude as blockchain[3]. In this work smart contract[1] is the major theme of the system it created two modules using solidity[3,4] language they are namely administrator, student as shown in the Fig.3 as web interface.

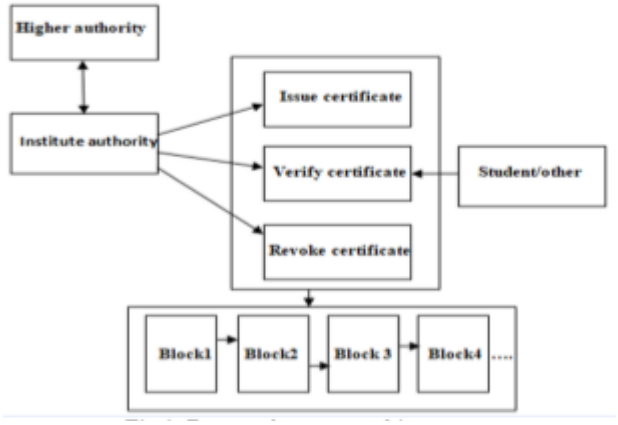

Fig. 1. Proposed system architecture

Administrator module: In this module the administrator can perform three functions such as

- Issue():
  This function is used to generate a new certificate to perform this action administrator should use admin login and use an account generated by testrpc.
- Verify()
  This function checks the existence of the certificate in blockchain network. If the certificate exits in the network then the system replies true as shown in Fig.7 or it shows false if certificate does not exist.
- Revoke()
  Revoke function in our system shows the certificate details such as certificate type, issuer name, recipient name and date of the certificate issued.

As shown in the Fig.4 Metamask [11] login is required because it is a web injection that carries the asset required for certificate generation. Administrator is ready to generate certificate he requires following details as shown in the Fig.5 like document id, certificate type, issuer name, and receiving person name. After filling all the fields admin should click the button to issue certificate then a new certificate is created with a timestamp [2] and Transaction details are stored in the network as shown in the Fig. 6. Issue certificate is payable operation for that gas price is chargeable following table.1, graph shows the gas price required for issue of the certificate.

Table- I: Representing the stats of certificates, total ether

No.of certificates	Gas Limit (units)	Gas Used	Gas Price CGWEI	Total ETH
1	20643	137622	100	0.0137622
10	206430	1376220	1000	1.37622
20	412860	2752440	2000	5.50488
30	619290	4128660	3000	12.38598
40	825720	5504880	4000	22.01952
50	1032150	6881100	5000	34.4055
100	2064300	13762200	10000	137.622

Student module: In this module there is only one function exist that to for checking the presence of the certificate in the blockchain. To perform the operation our system asks for the user document id that is similar to certificate number, certificate type, and receiver name as input if the certificate exists in the network the status of the certificate will be true, otherwise the status will be false as shown in the Fig-7.

Our system is scalable hence any number student can verify at the same time there is no concurrency.

The Fig.2 representing the graph between number of certificates issued for the ether consumed by the system. It clearly shows that direct proportionality because as increase in the certificates generated the total cost of the ether consumption also increases.

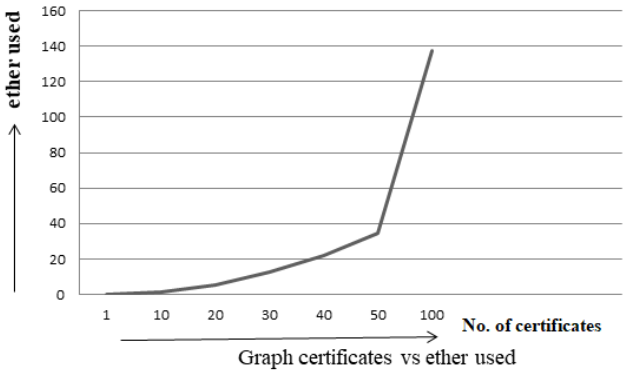

Fig. 2. Certificates Vs. Ether graph

IV. RESULTS AND DISCUSSIONS

Below Fig.3 shows the application window of the Administrator and student side credentials. It acts as an interface between blockchain based application level to the user's level.

Fig. 3. Admin, Student login modules

Metamask login is required to hold the asset in metamask[11] wallet. There fore Fig.4 is a security check to login testrpc generated seed phrase should be entered here for asset transfer to metamask wallet.

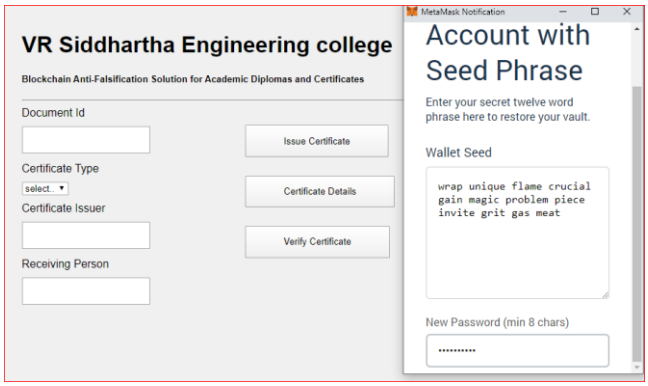

Fig. 4. Metamask Login

Cost of Gas value to generate a certificate also can visible in metamask screen as shown in Fig 5. This is a pop up message from metamask[11] whenever adminstrator tries to perfrom issue operation this dialog box comes as a system call it is also known as metamask notification. Here admin takes the decision of generating the certificate.

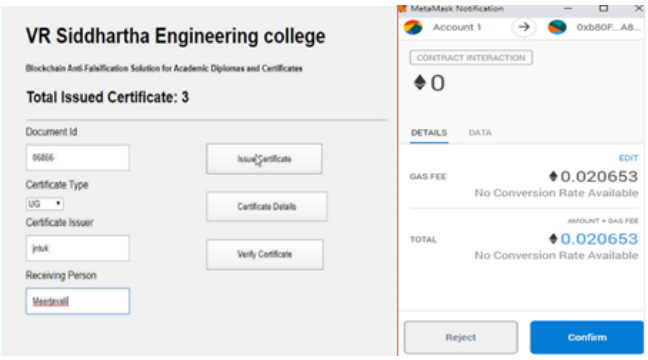

Fig. 5. Administrator issuing certificate using gas.

Fig.6 shows the Eth transaction details after issue of the certificate/creation of the certificates based on the input data given by the admin authority. These details appear at metamask side only.

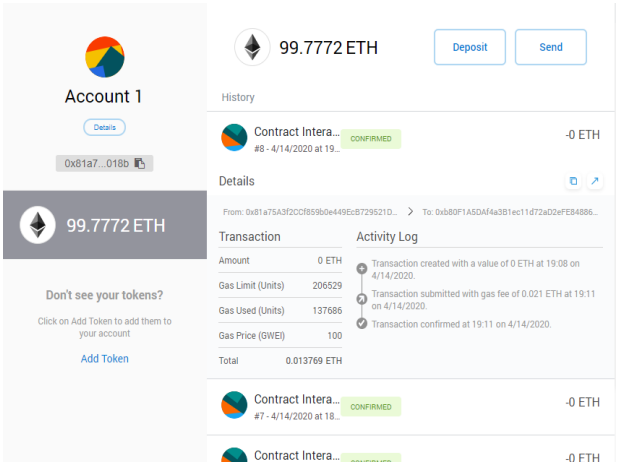

Fig. 6. Transaction details after issuing certificate.

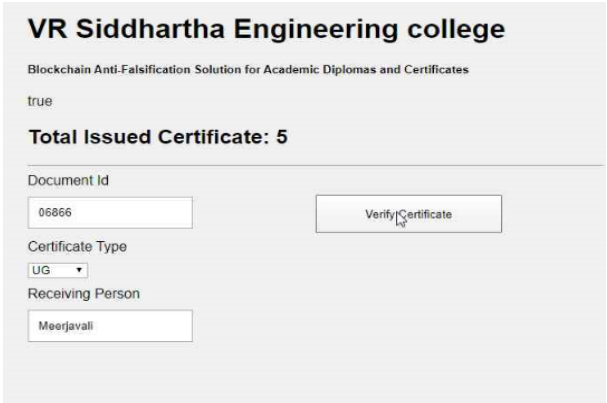

Fig. 7. Verifying certificate through student login.

The above Fig.7 the student side verify on blockchain platform. It will have only verification option. So if certificate has successfully generated at administration side then only can visible at this side. Verify is non-payable function hence it can be used for free to check the status of the certificate issued or not.

V. CONCLUSION

Data security is one of the major features of blockchain technology. Blockchain[1,3] is a large and open-access online ledger in that each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire about the information on any certificate from the system without any third parties dependency. There is no certificate loss , students also benefit with this system because there is always a protection to their certificate , they don't have any paper certificate to save and protect in their lockers blockchain network does this for them always from anywhere any time they can restore their certificate. Future work of this system to create a function which eliminates the fake certificates already exists in the society. In conclusion, the system assures information accuracy and security.

REFERENCES

1. T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates," IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 629-633.
2. A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar and P. C. K. Hung, "A Permissioned Blockchain-Based System for Verification of Academic Records," 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), CANARY ISLANDS, Spain, 2019, pp. 1-5.
3. J. Cheng, N. Lee, C. Chi and Y. Chen, "Blockchain and smart contract for digital certificate," IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051.
4. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," in IEEE Access, vol. 6,2018, pp. 51125127.
5. A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash and R. Pradhan, "A Distributed Credit Transfer Educational Framework based on Blockchain," Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), Allahabad, India, 2018, pp. 54-59.
6. Bae, S., Shin, Y. An Automated System Recovery Using BlockChain. In Tenth International Conference on Ubiquitous and Future Networks (ICUFN) ,2018,pp. 897-901.
7. S. Bae and Y. Shin, "An Automated System Recovery Using BlockChain," Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, 2018, pp. 897-901.
8. Zheng, Z., Xie, S., Dai, H. N., Chen, X.,and Wang, H. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, vol.14 no.4,2018,pp. 352-375.
9. Gas value for ethereum gas, https://blockgeeks.com/guides/ethereum-gas
10. Kanan, T., Kanaan, R., Al-Dabbas, O., Kanaan, G., Al-Dahoud, A., & Fox, E. Extracting Named Entities Using Named Entity Recognizer for Arabic News Articles. International Journal of Advanced Studies in Computers, Science and Engineering, vol.5, no.11, pp. 78-84.
11. https://www.trufflesuite.com/docs/truffle/getting-started/truffle-with met amask.
12. Z. Shae and J. J. P. Tsai, "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine," IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, 2017, pp. 1972-1980.
13. Q. Liu, Q. Guan, X. Yang, H. Zhu, G. Green and S. Yin, "Education-Industry Cooperative System Based on Blockchain," 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, 2018, pp. 207-211.
14. Kanan, T., Kanaan, R., Al-Dabbas, O., Kanaan, G., Al-Dahoud, A., & Fox, E. Extracting Named Entities Using Named Entity Recognizer for Arabic News Articles. International Journal of Advanced Studies in Computers, Science and Engineering, vol.5, no.11, pp.78-84.
15. M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, ³Proof-ofpersnonhood: Redemocratizing permissionless cryptocurrencies", IEEE Eur. Symp. Secur. PrivacyWorkshops (EuroS PW), Apr. 2017, pp. 23-26.

AUTHORS PROFILE

Mr. Meerja vali Shaik, pursuing 4/4 B.Tech in department of CSE at Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, AP. His area of interest in computer science, passionate towards learning new things.

Dr. Ch. Rupa, is working as a professor in VRSEC (A), Vijayawada. She was a senior member of IEEE and Life Member of CSI, ISTE, IAENG, IEI, IACSIT. She published more than 70 papers in various journals and conferences. JNTU kakinada has awarded her as a Young Engineer of 2010. IEI awarded her as National young Engineer of 2011 Govt of A. P and IEI by combined awarded her as Young Engineer of 2012. Her main research interests includes information security, Image Processing, Security algorithms. She has received couple of awards from IETE, IEI(I) for her work.

Mr. M N S Koundinya, pursuing 4/4 B.Tech in department of CSE at Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, AP. His areas of interest includes Computer networks, Database matainance and cyber security. Furthermore I am planning to do my master's in the field of computer science as there is more to explore

Mr. Rohith Gadde, pursuing 4/4 B.Tech in department of CSE at Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, AP. His area of interest includes Java Programming and Cyber Security and IoT.

Mr. Harish Donepudi, pursuing 4/4 B.Tech in department of CSE at Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, AP. His area of interest includes Internet Of Things, Cyber Security.