Journal of Advances in Mathematical & Computational Sciences
An International Pan-African Multidisciplinary Journal of the SMART Research Group
International Centre for IT & Development (ICITD) USA
© Creative Research Publishers
Available online at https://www.isteams.net/ mathematics-computationaljournal.info
DOI: dx.doi.org/10.22624/AIMS/MATHS/V9N2P4
CrossREF Member Listing - https://www.crossref.org/06members/50go-live.html

A Verified Ethereum-Based Smart Contract Model to Detect Counterfeit Educational Certificate.

Ahubele, B.O & Ndukwe, O.E.
Department of Computer Science
University of Port Harcourt
Port Harcourt, Nigeria
E-mails: betty_ahubele@uniport.edu.ng; ogeking2004@gmail.com
Phone: +2348087473122; +2347039119269

ABSTRACT

Counterfeit certificate is indeed a pervasive and chronic phenomenon that undermines the faith in academic institutions, costs a lot of money and hinders societal growth. Regrettably, costly, time-consuming and inefficient certificate verification solution is still in existence. It has become very difficult to distinguish between real and fake certificates. In a bid to get employed, young graduates who have no academic result or could not complete his or her career in engaging institution present counterfeit certificate to the employee. This could result in huge financial loss and employment of incompetency. Blockchain-based smart contract has emerged as a fruitful means of verifying educational certificates and combating document fraud and misuse. This paper presents a verification model to detect counterfeit certificate using blockchain-based smart contract model. We presented a model to save the society from the effect of certificate forgery by enabling a verified smart-contract against security vulnerability and to detect counterfeit certificate.

Keywords: Ethereum Virtual Machine (EVM), Counterfeit Certificate, Smart Contract Verification, Etherscan

Ahubele, B.O & Ndukwe, O.E. (2021): A Verified Ethereum-Based Smart Contract Model to Detect Counterfeit Educational Certificate. Journal of Advances in Mathematical & Computational Science. Vol. 9, No. 2. Pp 51-60.
DOI: dx.doi.org/10.22624/AIMS/MATHS/V9N2P4.
Available online at www.isteams.net/mathematics-computationaljournal.

1. INTRODUCTION

Certificates issued by major degree awarding institutions are in paper form and the contents of the paper can be easily manipulated due to technological advancement. This consequently poses a threat to those institutions that issues the certificate and the organization that the certificate owner intends to submit the obtained certificate for employment opportunity. Verification process is necessary to combat certificate fraud. Document verification is a complex domain with a lot of difficult and time consuming methods. Various types of documents, such as financial paper, government policy paper, transactional paper and educational certificates may require automated verification and authentication process [17]. To carry out certificate verification, some academic centers allow a simple and fast online query to verify the authenticity of employer's certificates. Some implore the sources of a third party either by default or as required by regulations to verify the presented certificate [5]. A predominant problem today is the number of fake certificates in circulation. Due to digitization, blockchain emerged as a great potential for authenticating educational certificate enabling a secure and efficient digital certificate validation [15]. Blockchain-based systems for academic certificate have shown greatly improved potential to overcome the inherent limitations of paper or web-based system.

The problem of counterfeiting certificates has become a menace which geared various research articles on building smart contracts for the digital certificates. In [9] a smart contract was developed for digital certificates to solve the problem of forgery. The electronic file of the paper certificate was generated and the hash grade computed and stored on the blockchain. In another paper, [10] worked on preventing difficulties in managing traditional paper testimonials by developing an ethereum based smart contract certificate system. Increased adoption of smart contracts requires strong security. Sadly, it becomes a challenge to create bugs free smart contract as critical vulnerabilities are discovered and exploited. The correctness of execution as well as security is necessary to keep business process smart contracts secure. In this paper, we carried out the smart contract verification for functional requirements before deploying on the Ethereum Virtual Machine (EVM). The proposed system is a functionally corrected and secured certificate verification model.

2. PREVIOUS WORKS

Recently, there has been a paradigm shift in the issuance of certificate using online platform. Blockhain technology creates a cryptographically secure and shared ledger for digital transactions. The usability of blockchain solutions has hit 5.27 billion unique phone users by a large number of mobile devices and applications [4]. In [1] two permissionless platforms such as ethereum and Bitcoin were used for certificate verification. The authors also proposed which helps to verify a user real identity through a QR Code and generate a certificate that is time saving. As the number of universities, college of education, polytechniques and so on are increasing, certificates have become a problem for those institutions. Tis need a sharp solution. [2] presented a reliable and secure method for verifying graduates credentials utilizing blockchain. The study enabled digital storage of genuine certificates and verification when needed without time wastage. The authors used ethereum test network and the test results generated a secure and feasible solution o online certificate management system.

Furthermore, employer needs to verify the originality of the certificate presented by his employee. The need to provide a time effective mechanism in order to authenticate the certificate from issuing institution arises. Similarly, [3] proposed a verification system using blockchain. The presented system is an anti-forged mechanism for educational certificates. To eliminate the issue of certificate forgery, the authors also provided a model to enable the storage of educational certificate in digital format. This yielded an immutable digital certificate in Ethereum-based blockchain. [5] designed a digital signature scheme and timestamp for education degree fraud detection and certificate verification using blockchain. The proposed system is a two-way balanced verification system which facilitates certificate checks for students and authenticity heck of certificate from trusted source during employer recruitment. The authors adopted a digital signature technology to solve the present certificate verification system to end fraud and promote transparency in the educational system.

Educational certificates is said to have more value which results in people producing fake certificates for individual esteem and in pursuit for job. However, [16] utilized Hyperledger permissioned blockchain in verifying educational certificate. The model uses encryption API which grants access to only those with assigned unique identify to the hyperledger platform. The ownership is preserved by linking the owner's document with its unique identity. Certificate verification is carried out by ensuing confidentiality and privacy of the owner.

3. BLOCKCHAIN TECHNOLOGY

In 2008, a pseudonym named Satoshi Nakamoto proposed the concept of blockchain by publishing his white paper named "Bitcoin: a peer-to-peer electronic cash system [14]. Blockchain is a distributed ledger which helps to solve the problems of centralization by providing a platform for programs to be run on its virtual machines. To provide features such as transparency, security, decentralization, immutability etc., blockchan utilizes mechanisms such as consensus protocols and cryptographic techniques. Each block consists of records which are linked together creating transaction hash value using hashing technique (SHA 256). Different data are recorded in distinct blocks and allow verifications to be made without the service of a third party. All distributed nodes form a timestamp blockchain. The data stored in each block can be verified simultaneously, transparent, secure, and immutable and open to the public once entered [8]. The emergence of Ethereum Smart Contracts in 2013 brought about the innovation of blockchain 2.0. As presented in Fig. 1, blockchain 1.0 focused mainly to solve problems concerning cryptocurrencies and decentralized payments by Bitcoin to Blockchain 2.0 which was adopted for the decentralization of digital assets through smart contracts.

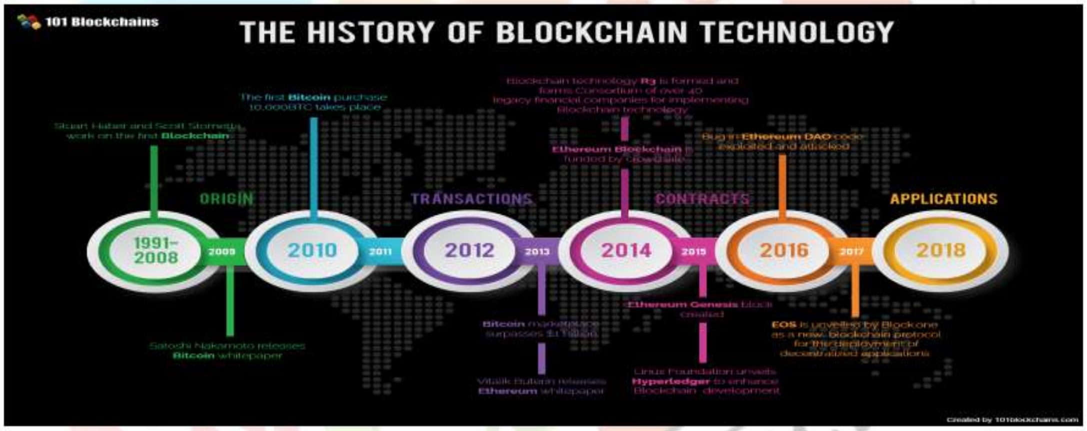

101 Blockchains
THE HISTORY OF BLOCKCHAIN TECHNOLOGY
Stuart Haber and Scott Stornetta work on the first Blockchain
The first Bitcoin purchase 10,000BTC takes place
Blockchain technology R3 is formed and forms Consortium of over 40 legacy financial companies for implementing Blockchain technology
Ethereum Blockchain is funded by crowdsale
Bug in Ethereum DAO code exploited and attacked
ORIGIN
TRANSACTIONS
CONTRACTS
APPLICATIONS
1991–2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Satoshi Nakamoto releases Bitcoin whitepaper
Bitcoin marketplace surpasses $1 billion
Vitalik Buterin releases Ethereum whitepaper
Ethereum Genesis block created
Linux Foundation unveils Hyperledger to enhance Blockchain development
EOS is unveiled by Blockone as a new blockchain protocol for the deployment of decentralized applications
Created by 101blockchains.com

Figure 1: History of Peer-to-Peer Blockchain [11]

4. THE ETHEREUM VIRTUAL MACHINE (EVM)

The first or initial generation of blockchain was designed to solve the problem of crypto-currency. As blockchain technology began to garner huge impact in diverse industries, the Ethereum blockchain was developed to provide support for implementing smart contracts or decentralized application. These smart contracts represent the basis for true ownership of digital assets and a range of DApps (Decentralized Applications) [13]. EVM is the operating system on which business process runs. Solidity was developed as a JavaScript-like programming language for building contract codes that executes on EVM.

The Solidity compiler translates this code into EVM bytecode which is sent to the Ethereum network as a transaction to be given its own address. Figure 2 shows how an Ethereum-based smart contract works. A contract address consists of its own storage state data) and an amount of 'ether' balance (i.e ethereum token). The Ethereum currency "Ether" was inspired by Bitcoin, but what makes this platform different is the support for smart contract execution. Smart contracts represent automated business process logic that can send and receive transactions, giving developers the leverage of high auditability, availability, transparency, and independency.

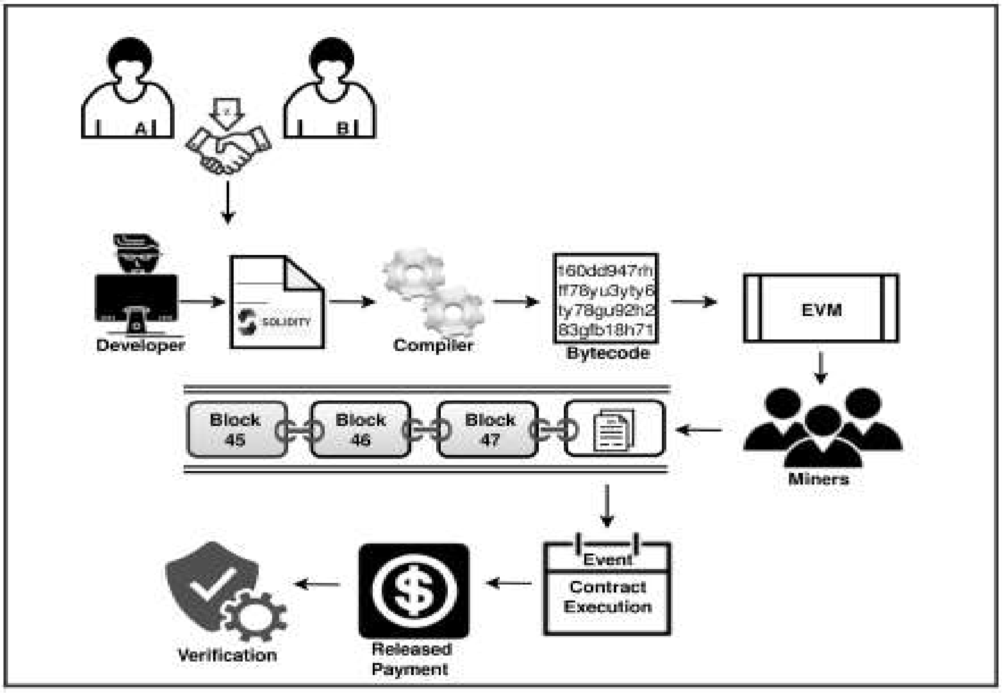


Figure 2: How Ethereum Smart Contract Works [7]

5. THE PROPOSED SYSTEM

The existing blockchain platform for certificate verification utilizes Ethereum Virtual Machine (EVM). The current implemented smart contract lack verification for functional requirements and run time error check. In our study, the smart contract will be verified before deployment on the EVM. This will enable the institution and contractual parties to review contracts source code for loophole and vulnerability which the hacker may exploit to launch an attack. Moreso, it is very pertinent to carry out a review of smart contract source code by the parties as contract deployed on the blockchain cannot be altered. A verified smart contract also ensure system specifications and functional requirements are met. Issues underlying the design and implementation of decentralized smart contract are our major goal. The primary goal of this system is to execute an error free smart contract against security vulnerability on the blockchain and also for verifying educational certificates.

6. SYSTEM DESIGN

In this paper, a blockchain-based smart contract for certificate verification was developed and programmed on Ethereum (EVM) platform. The system consists of three modules which include the student registration, E-Cert platform and Smart contract verification. Firstly, the student registers on the online school certificate application platform, requesting for electronic certificate. The student's request is then reviewed by the institution and approved if details provided by checking with the school's IPFS are authentic. Once the information of the graduate has been entered by the E-Cert module, the QR Code and the certificate serial number will be generated. The student's QR Code links his identity and the certificate on the electronic platform.

The issuing applications are responsible for the business logic which includes certificate requesting, examining, signing and revocation of certificates. The system is designed to record the transaction hash of the certificate on the blockhain. Lastly, the E-Cert smart contract is created using solidity programming language. The contract source code is verified using etherscan blockchain explorer tool to determine if functional requirements are met and to prevent loophole or possible vulnerability for a hacker to launch an attack. Upon confirmation, the E-Cert contract is executed and deployed on the blockchain. The companies also send enquiries to the system and are informed if the serial numbers are validated. The QR Code detects if the certificate has been manipulated. Validated certificates will be forever valid regardless of the existence of the certificate issuance institutions.

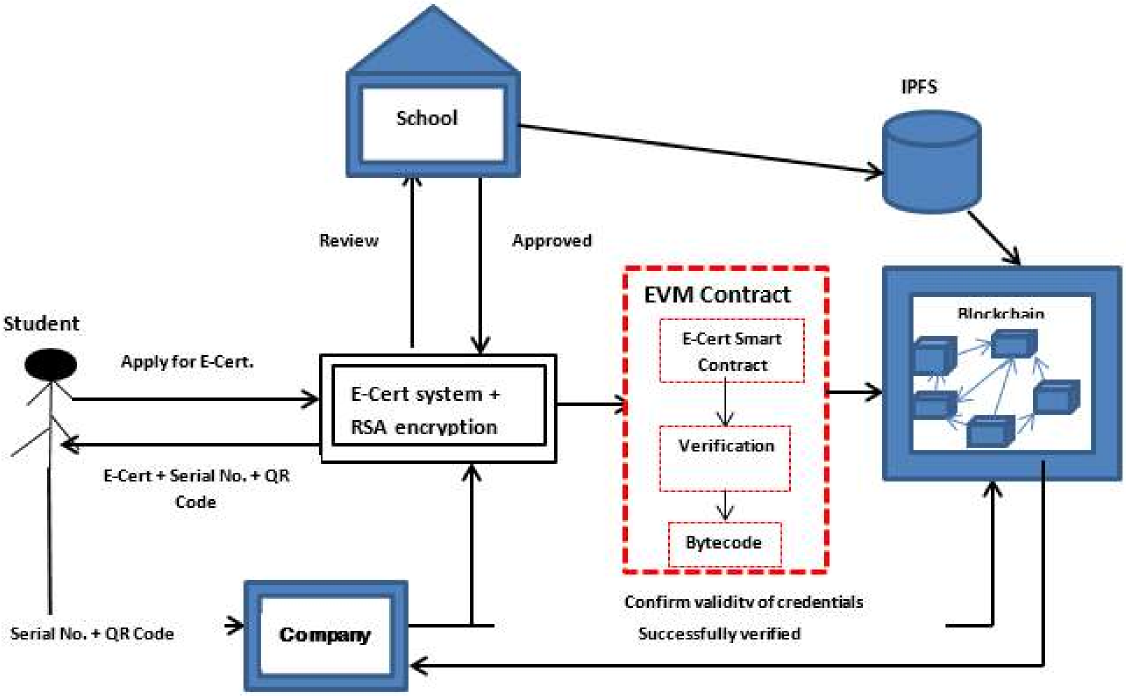


Figure 3: The Proposed System Architecture

7. THE SYSTEM PROCESS FLOW

Ethereum Blockchain is a decentralize application that supports programming. The working processes of the proposed system are as follows:

1. The students apply for degree certificate
2. Schools review request and grants certificate if approved.
3. E-Cert system generate QR Code and Certificate serial number
4. Smart Contract of the –Cert system is developed and verified using Etherscan blockchain verification tool.
5. Smart contract meets specification and functional requirement and deployed on EVM
6. Verification can be done by the company from the data stored in the blockchain.

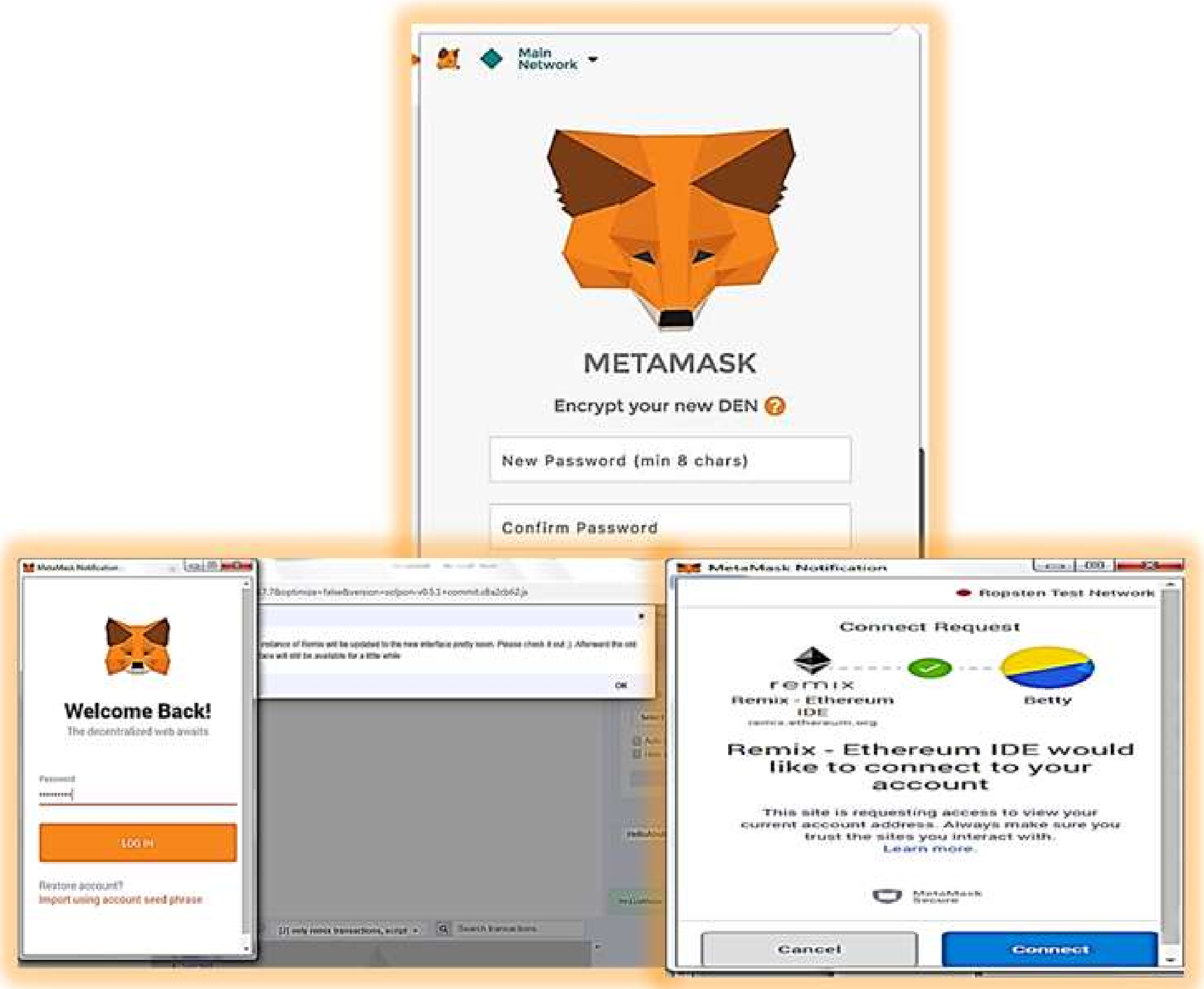
8. THE POPOSED SYSTEM BENEFITS

Education providers will be able to give the formal certificates providing proof of the completion using blockchain technology. The following are highlighted advantages of the designed system:

i. Our proposed model has smart contract which potentially helps to automate transactions and boost business productivity.
ii. The smart contract is verified to detect any loophole and vulnerability, meeting functional requirements and business decision.
iii. Counterfeit certificate can be traced by the employee without involving a third party intermediary.
iv. Blockchain-based certificate verification helps to eliminate inefficiency, error and time wastage prominent with traditional paper-based method.

9. RESULTS AND DISCUSSION

Figure 4 shows the smart contract development tools (MetaMask login screen and Remix IDE). MetaMask serves as an ethereum wallet and an interface which allow users to interact with smart contracts and DApps on the web without installing an Etheruem Node. Advanced developers can install and use Solidity Compiler but the Remix IDE provides a pre-installed environment. It is only required to add MetaMask as a Chrome Extension in order to create a wallet and acquire Ether through the Ropsten, Kovan and Goerli test networks to execute the transaction. Once MetaMask is successfully added to Chrome extension, an existing wallet can be imported by entering the appropriate private key or importing the pass phrase from its JSon file. A new wallet can also be created by generating a unique password and the Passphrase for the wallet. During the process of creating the Metamask wallet, the password is created and the account secret backup phrase that can be used for backing up and restoring the account is also created and saved. Disclosing or sharing an account password or pass phrase can be a security risk on the wallet. The account detail can be written on a piece of paper securely or stored safely on an external encrypted hard drive for safety. However to execute the transaction, real Etheruem must be purchased as it is needed to run the smart contract on the mainnet.



METAMASK

Encrypt your new DEN

New Password (min 8 chars)

Confirm Password

Welcome Back!

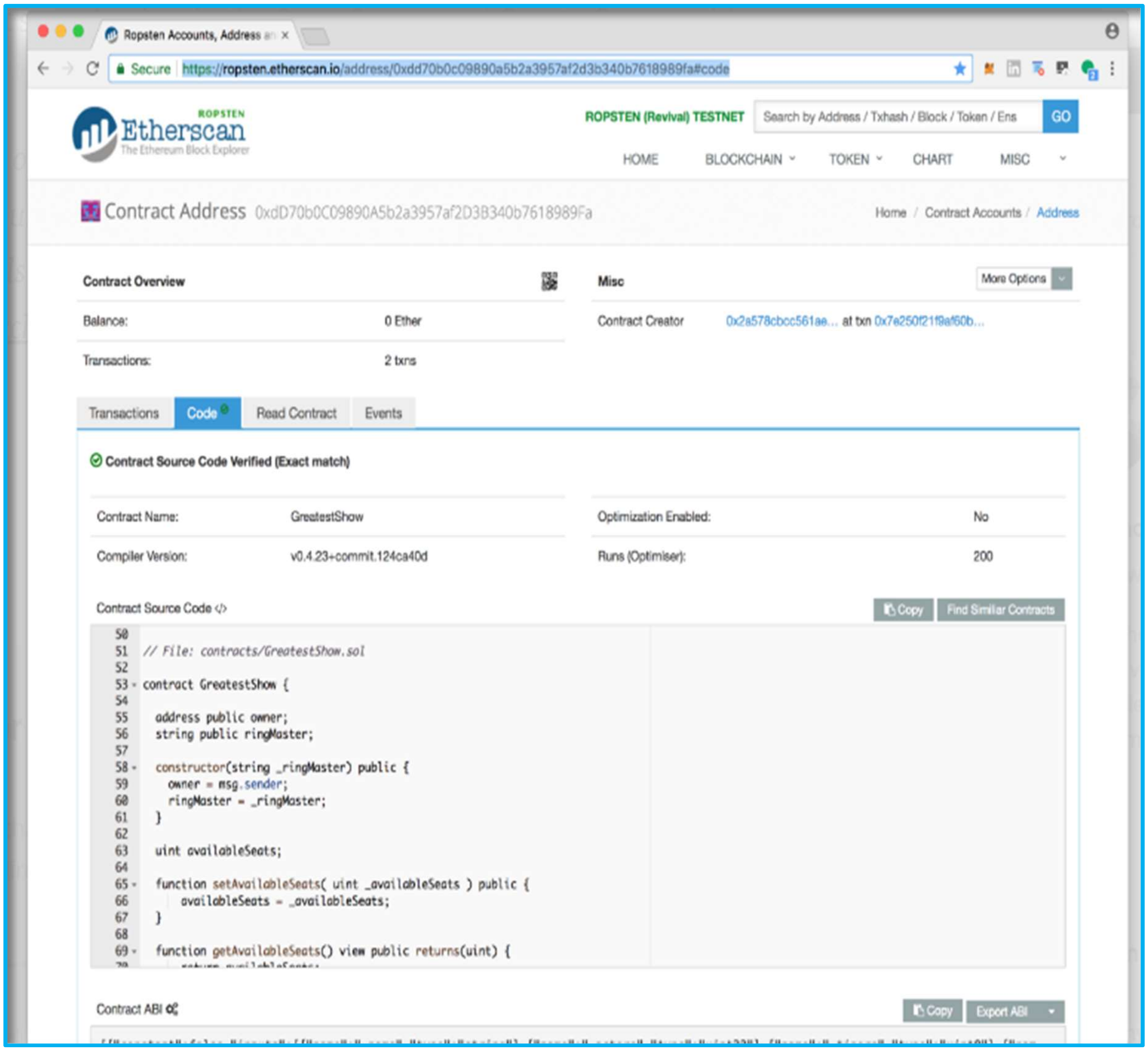
The decentralized web awaits

Remix - Ethereum IDE would like to connect to your account

This site is requesting access to view your current account address. Always make sure you trust the sites you interact with.

Figure 4: Smart Contract development tools

Smart contract verification and validation is a unique feature with EVM. Figure 5 shows how to verify and publish a transaction on etherscan. Etherscan is the most popular blockchain explorer where contracts can be verified and published. It is very pertinent to verify smart contracts in order to show that the contract code is exactly what is being deployed onto the blockchain and also allows the public to audit and read the contract. Once the contract source code is entered, the Contract bytecode will be automatically displayed on the verification page too. Etherscan is intended to help clients in cooperating with any smart contract sent onto the Ethereum blockchain. To guarantee further security, users are just ready to cooperate with smart contracts that are verified on Etherscan. Verified contract implies that the contract code given by the proprietor of the contract coordinates the contract code sent onto the Ethereum Blockchain.


Ropsten Accounts, Address an
Secure
ROPSTEN
Etherscan
The Ethereum Block Explorer
ROPSTEN (Revival) TESTNET
Search by Address / Txhash / Block / Token / Ens
GO
HOME
BLOCKCHAIN
TOKEN
CHART
MISC
Home / Contract Accounts / Address
More Options
Transactions
Code
Read Contract
Events
Copy
Find Similar Contracts
Copy
Export ABI

https://ropsten.etherscan.io/address/0xdd70b0c09890a5b2a3957af2d3b340b7618989fa#code

Contract Address 0xdD70b0C09890A5b2a3957af2D3B340b7618989Fa

Contract Overview

Balance:	0 Ether
Transactions:	2 txns

Misc

Contract Creator 0x2a578cbcc561ae... at txn 0x7e250f21f9af60b...

Contract Source Code Verified (Exact match)

Contract Name:	GreatestShow	Optimization Enabled:	No
Compiler Version:	v0.4.23+commit.124ca40d	Runs (Optimiser):	200

Contract Source Code </>

```

// File: contracts/GreatestShow.sol

contract GreatestShow {

  address public owner;
  string public ringMaster;

  constructor(string _ringMaster) public {
    owner = msg.sender;
    ringMaster = _ringMaster;
  }

  uint availableSeats;

  function setAvailableSeats( uint _availableSeats ) public {
      availableSeats = _availableSeats;
  }

  function getAvailableSeats() view public returns(uint) {
      return availableSeats;
```

Contract ABI

Figure 5: Smart Contract Verification using Etherscan tool

10. CONCUSION AND FUTURE RESEARCH

Information technology has transformed data innovation; internet accessibility and the constant use of cell phones have changed societal way of living. Data security is an important feature of blockchain technology. Blockchain is a large and open-access distributed ledger in which every node saves and verifies the same transactional data. Using the proposed verified ethereum-based smart contract model will ensure that the system is designed according to specifications and the functional requirements are met and also reduces the possibility of counterfeit certificate.

The process offers an open and transparent access to certificate application and automated certificate. Companies can thus inquire for information on any certificate presented by the employers. Blockchain has facilitated recognition of learning, certification of both formal and informal learning. Globally, governments, enterprises, and start-ups are exploring the blockchain in a wide variety of use cases and for a wide variety of requirements and regulatory demands. However, there is still much that is unknown about the development of the trusted blockchain-based systems. In the future, it is required to improve users' knowledge on how to create a workable blockchain-based systems and evidence that blockchain-based systems will work as expected.

REFERENCES

1. Sifat, N.B., F. Hossan, R. Pollole, N.N. Abir A.Z Zarin and M.F. Miridha. Blockchain-based Architecture for Certificate Authentication. International Conference of Innovative Computing and Communication(ICIC)2021. https://dx.doi.org/10.139/ssrn.3482788.
2. Reddy T.R., P.V.G.D. Prasad, R. Srinivas, Ch.V. Pagbavandiran, R.V. Lalitha and B. Annapurna. Proposing a reliable method for securing and verifying credentials of graduates though blockhain. EURASIP Journal of Information Security. 7(2021).
3. Kumar D.K., P. Santhil and M.D.S Kumar. Educational Certificate Verification System using Blockchain. International Journal of Scientific and Technology Research (IJSTR). 2020. 9(3). 82-85.
4. Kepios. Digital Around the Wold. Data Reportal-Global Digital Insights. 2021. https://datareportal.com/global-digital interview.
5. Jayesh, G.D, Dr. K.T. Patil, S.M. Tikan & V.B. harat. Edcation Degree Fraud Detection and student Certificate verification using blockchain. International Journal of Engineering Research & Technology (IJERT). 2021. 9(7). 300-303.
6. Rajesha, R., K. Mohite, S. Sahana, B.N. Shilpasree and K.R. Rakeh. Counterfeit Detection of Documents using Blockchain. International Journal of Engineering Research & Technology (IJERT). 10(7). 358-361.
7. Sayeed, S., H. Marco-Gisbert & T. Caira. Smart Contract : Attacks and Protections. IEEE Access. 2020. Di:
10. 110/Access.2020.2970495.
8. Zhenzhi Qiu. Digital certificate for a painting based on blockchain technology. Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
9. Zheng, Z., S. Xie, H. Dai, X. Chen and H. Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017. 557-564. Doi:10.1109/BigDataCongress.2017.85
10. 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: 10.1109/IOTM.0001.1900094.
11. Hargude, C.R. G. Ashutosh, A. Nawale and S. Adsure. Verification and Validation ofCertificate using Blockchain. International journal of Creative Research Thought (IJCRT). 2021. 9(6).714-718.
12. Keerthana, T., Tejaswini, R., Yamini, V., & Hemapriya, K. (2019). Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract. International Journal of Research in Engineering, Science and Management. 267-270. https://www.ijresm.com/Vol.2_2019/Vol2_Iss3_March19/IJRESM_V2_I3_70.pd

13. Bang, T., H. Hoang, D. Nguyen, T. Trien & T. Quan. Verification of Ethereum Smart Contract: A Model Challege Appoach. International Journal of Machine Learning and Computing (IJMLC). 2020. 10(4).588-593.
14. Nakamoto, S.Bitcoin: A Peer-to-Peer Electronic Cash System.2008. www.bitcoin.org
15. Rayesh G.D, Dr.K.T Patil, S. M.Tikam and V.B.Gharath. Education Degree Fraud Detection and Student Certificate Verification using Blockchain. 13 July 2020. International Jounal of Engineering Research and Technology. www.ijert.org,
16. Omar, S.S, O. Ghazali, M.E Rana:A blockchain-based framework for educational certificates verification. Article in journal of critical reviews, 2019.
17. Mara,P and R.K Motupalli. Blockchain-based model to track and verify official certificates. International Journal of Engineering Technology and Management (IJETMS). 2022. 6(1). 7-15.