International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017),e-ISSN:2455-2585
International Conference on
Recent Explorations in Science, Engineering And Technology (ICRESET'19)
Volume-5, Special Issue-March, 2019.

CERTIFICATE ISSUING AND VERIFICATION USING BLOCKCHAIN

[1] Sathish R M.E.,(phD) , [2] Nilavann S , [3] Gopi K

[1] Assistant professor, Department of information technology
[2 3]UG Scholars, Department of information technology
[1 2 3]KGiSL institute of technology, Coimbatore

ABSTRACT -We are going through a very exciting phase of technological transformation. Blockchain _community is re-designing a lot of existing use cases and trying to solve a lot of unsolved use cases with the help of decentralized, peer-to-peer technology. A Certificate is a report that guarantees that an individual has gotten explicit training or has breezed through a test or arrangement of tests. Counterfeit testaments is a gigantic issue in our Nation. Even a unique paper testament can be forged easily. Verification check is a tiresome and time-consuming process for Organizations/Institutions. We propose a Blockchain(Distributed Ledger Technology) based solution for this problem with Distributed storage(IPFS). Thus certificates will be tamperproof, confidential and secure. Here, we are going to use Ethereum Blockchain. In this way, the Institutions will create the certificate with student information (such as StudentName, Student ID, NationalID, Degree, College, and other information)The system will commit transactions considering certificate as a digital asset and store them on IPFS with public key encryption. Hash of the certificate is stored in the blockchain. Only the certificate issuing authority/institute can create and issue the certificate. From that moment, the student becomes the owner of the certificate (digital asset). Whenever a Students wants to share his/ her certificate, they encrypt it with recipient public key, store it in IPFS and send the hash to recipient.Only the mapping of the digital assets will be present in the blockchain hus digital assets are encrypted and stored in IPFS.

Keywords - Cryptography, Smart contract, Distributed ledger technology(DTL) , IPFS Ethereum ,

Introduction

Blockchain is the backbone Technology of CryptoCurrency such as BitCoin. The blockchain is a immutable distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Now a days the blockchain technology is called as DLT (Distributed ledger technology).Simply Blockchain is an append only Data structure maintained by a network where each node in the network contains a copy of the blockchain and uses a consensus to decide which block should be accepted next.Thus in Bitcoin blockchain the system states are transaction of coins from one account to another. But blockchain can be used to store User defined state machines thus its use case grow beyond cryptocurrencies where it can be used in Finance Industries, Supply chain, Fraud detection and many other Industries.Smart contract are self executing contracts In this format, contracts could be converted to computer code,stored and replicated on the system and supervised by the network of computers that run the blockchain and change the state.The Blockchain can be permissioned network, Permissionless network, Hybrid Networks.

Cryptocurrencies uses a Permissionless network where anyone can join, Participate and see the transactions in the network.The permissioned network in which only the Authorized entities can participate.Hybrid network where it contains properties of both permissioned and permission less network.

Problem Statement

Storing the school/university/board certificates is a recurring process. For the Organization, verifying the authenticity of the certificates is tedious and cumbersome.The proposed solution will help the institutions to store the certificates in the decentralized way using the Blockchain system and give access to any organizations or any institution with the consent of the individual. sharable decentralized storage using digital signature and access.

Existing System

The current certificate issuing process is in the form of paper certificates so it can forged easily.Even though they use certain identity number to verify certificates the certificate forgery is not eliminate completely.For organizations and institutions the certificate verifying becomes a tedious process so they are seeking a better way to perform this task.

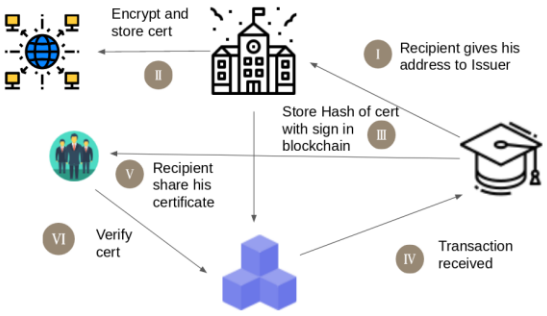
If a person lost his/her certificate then reissuing of the certificate take some time and a long process.

Proposed System

The system we propose is to make the Certificate digitize and store them in a Distributed ledger. So the recipient can share certificates digitally and the verifier can verify at any time in the distributed ledger.

Here the blockchain provides the distributed storage and security by using cryptography(Hashing and Digital Signature).Thus the issuer issue the certificate as a transaction to the recipient address with signature then recipient can use the unique transaction id to share certificate and verifier can verify certificate in the blockchain Features provided by our system Tamper-proof, Immutable, Autonomous using Smart contract, decentralized, no single point failure.

Architecture Diagram


Encrypt and store cert
II
Recipient gives his address to Issuer
I
Store Hash of cert with sign in blockchain
III
Recipient share his certificate
V
VI
Verify cert
Transaction received
IV

A FIELDS IN EACH MODULE

Recipient module

1 share certificate

2 view certificate

Issuer module

1 Issue certificate

Validator module

1 validate certificate

2 view certificate

Crypto Module

1 encryption of certificate

2 decryption of certificate

IPFS Module

1 Add certificate

Module Description

Recipicent module

The Recipient was only sharing and viewing the certificate

Issuer module

The work of an a issuer is to signature the certificated and encrypt it then store in blockchain

Validator module

The work of an a validator is checking for your certificate and view the certificate

Crypto Module

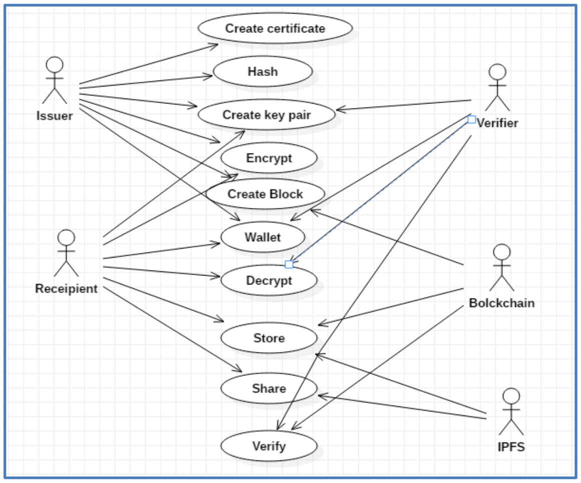
The Encryption and decryption work is done on the crypto module

IPFS Module

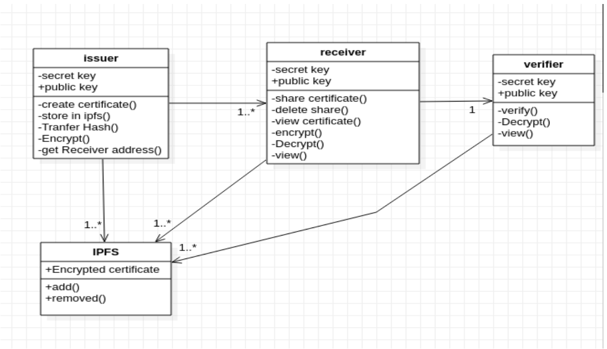
The IPFS (InterPlanetary File System) is only for append the certificate. We can't delete the certificate.

Diagrams

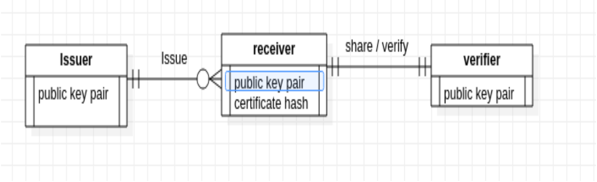
Use case diagrams



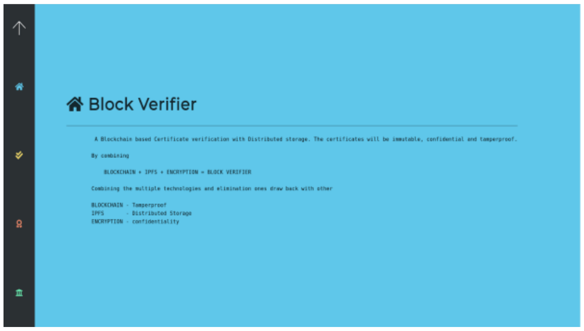
Class Diagrams



ER Diagrams



1. **Block Vertifier**

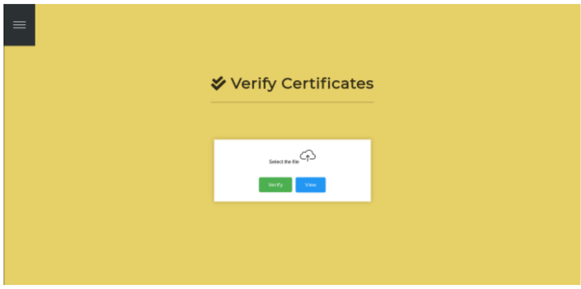


Block Verifier

```
 A Blockchain based Certificate verification with Distributed storage. The certificates will be immutable, confidential and tamperproof.

By combining

   BLOCKCHAIN + IPFS + ENCRYPTION = BLOCK VERIFIER

Combining the multiple technologies and elimination ones draw back with other

BLOCKCHAIN - Tamperproof
IPFS       - Distributed Storage
ENCRYPTION - confidentiality
```

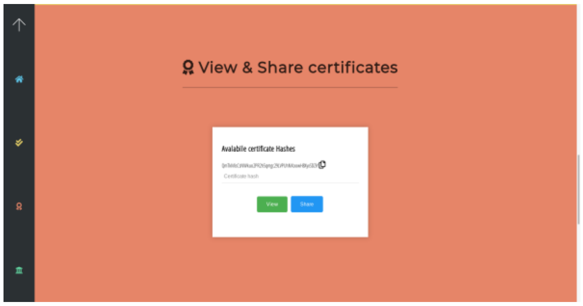
This module gives the basic information about our project Block Verifier how the Blockchain technology has been utilized, how security is provided to certificates in IPFS since the content can be access by anyone.sum information should be there in block verifier.the block verifier was used to easily to understanding propose about the blockchain technology in this module there in blockchain , IPFS and encryption method.the blockchain is tamper proof methodology. The IPFS is decentralized storage area.Confidentiality is the protection of personal information.Confidentiality suggests that keeping a consumer's data between you and also the client, and not telling others as well as co-workers, friends, family..

2. **Verify certificate**



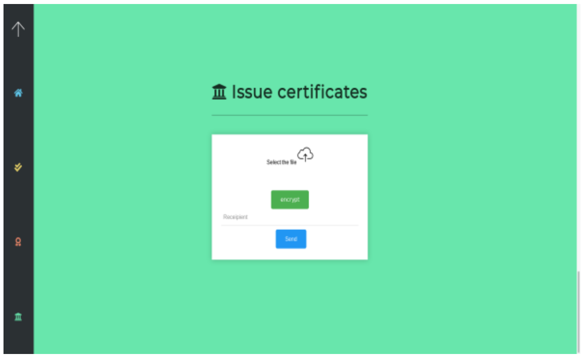
Verification module in which the Verifier (the person who wants to verify certificate) can able to upload the certificate they received from the recipients. Then they can able to verify the certificate by calculating the hash of the certificate and checking the certificate availability in the blockchain. The verification process only takes seconds to verify the certificate by comparing the calculated hash with hash in Blockchain.The verifier does not need to login in order to verify the Certificates. The validator calculate hash using the recipient certificate and compare the hash with the hash stored in blockchain. If the comparison matches then the certificate is valid one or else if is not a valid one. The recipient was sharing the certificate for any social media.

3. View and share certificate



Recipient module which is used by the recipient in order to see all the certificates they received as a transaction from the different Issuers. All the available certificate hashes will be displayed once he logged into the Metamask.All these hashes are calculated after the certificate are encrypted with the user public key. The IPFS was content based searching method.So however access the certificate with this hash other then the recipient cannot able to decrypt it. He can able to view the certificate and share it with others via Facebook, Google, others or Download it.the recipient only have the hash value.the ipfs is content based address system ones the transaction will be done. The recipient was decryption the certificate using Recipient public key

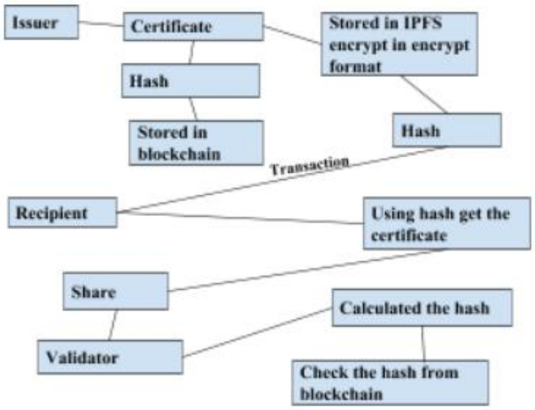
4. Issue Certificate



The Issuer module issuer can able to upload the certificate that he wants to issue to a recipient and then he needs to specify the recipient public key. Then by clicking the encrypt the certificate will be encrypted with the recipient public key. On press, the send key the certificate will be added to the IPFS also the digital signature and hash of certificate will be added to Blockchain then the certificate hash will be sent to the recipient as a transaction.the issuer can be only issuing the certificate and upload in hash from the blockchain it was encrypted by recipient public key.the hash will be sending the recipient for one transaction.the recipient was only the hash. The hash contains the address

Data flow diagram

The issuer create the certificate for the recipient and create the hash from the certificate and stored hash in blockchain. The certificate is stored in encrypted format using recipient public key.


Issuer
Certificate
Stored in IPFS encrypt in encrypt format
Hash
Stored in blockchain
Hash
Transaction
Recipient
Using hash get the certificate
Share
Calculated the hash
Validator
Check the hash from blockchain

The encrypt hash form the IPFS is transacted to the recipient and recipient uses the hash to view the certificate to validator. The validator calculate hash using the recipient certificate and compare the hash with the hash stored in blockchain. If the comparison matches then the certificate is valid one or else if is not a valid one. The recipient was sharing the certificate for any social media.

Conclusion

We have proposed a certificate issuing and verification system using the distributed ledger technology(DLT). Our project uses blockchain for authenting the certificate and share it securely using IPFS(InterPlanetary File System) The certificate stored in IPFS. only a recipient view the certificate.if it is the recipient was sharing the certificate for any social media. The IPFS to have the certificate. In this certificate was encrypt format and the store in IPFS. We are using the public key encryption..

REFERENCE:

[1]Satoshi Nakamoto ,"Bitcoin: A peer-to-peer Peer-to-Peer Electronic Cash System" 2008.

[2]S.Eskandari, D.Barrera,E.stobert and j.clark "A first look at the usability of bitcoin management" (at ArXiv in 2015)

[3]Mr. Hari Krishna K Ms. Aaradhana Deshmukh Mrs. Vaishali Maheshkar Dr. N.M. Nandhitha Bhupendra Pratap Singh "Tendermint:blockchain app development simplified" (2017)

[4] POA Ethcore,"Parity:Nextgeneration ethereum browser" (2017)

[5] M.castro and B.Liskov "practical byzantine byzantine fault tolerance" (545 Technology Square, Cambridge, MA 02139)

[6] "Hyperledger , Sawtooth distributed ledger" 2016

[7] "Ethereum blockchain app platform" 2017

[8]"untangling blockchain, A data processing view of blockchain system" (2018)

[9]Marko Vukolic "The quest for scalable blockchain Fabric: proof of work vs BFT replication "(conference paper may 2016)

[10]MassimoDiPierro(Journal&Magazine:Computing in Science & Engineering in 2017)

[11] Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda,Víctor Santamaría(Journal & Magazine:IT Professional in 2018)

[12]Brian A. Scriber "A Framework for Determining Blockchain Applicability" (Journal & Magazine: IEEE software in 2018)