ISSN No:-2456-2165

CryptoID - Blockchain Powered Digital Identity Cards

Abdul Basit Hakimi
Department of Computer Science and Engineering
ITM sls Baroda University
Vadodara, India

Madonna Lamin
Department of Computer Science and Engineering
ITM sls Baroda University
Vadodara, India

Abstract:- This paper proposes a system to generate secure and reliable identity cards for educational institutes or organizations which are issued to the student or employee respectively. The proposed application design ensures that no duplicate or fake identity cards of institution/organization are possible to generate. The design removes the problem of portability issues associated with physical identity cards.

Keywords:- *DAPPs, Secure Identitycards, Blockchain, Metamask, Ethereum, I Pfs.*

I. INTRODUCTION

Blockchain provides a secure, privacy-preserving and scalable way of exchanging verified digital credentials between two parties. Ethereum expands the limited capabilities of the blockchain and allows developers to create robust decentralized applications also called Dapps.

Decentralized applications or Dapps are softwares that communicate with the blockchain, which manages the state of all network entities. The advantage of Dapps is that values in the blockchain cannot be modified by anyone, person or entity.

Metamask allows users to run Ethereum Dapps on their browser with a secure identity vault. It provides a user interface to manage the identities of different sites and sign blockchain transactions, making Ethereum applications more accessible and easier to use for all.

Identity cards are essential credentials for individuals to identify that they belong to an educational institute or organization. They help in authorization of certain confidential aspects of institutes or organizations and in case of any suspicious activity that may occur within the premises the log of the authorization is considered to catch hold of the guilty. With the boom of online transactions there has been an uprising of frauds and harmful cyber security attacks in institutes or organizations like creation of fake identity cards, changing the database or logs to acquire access to premises and perform malicious activity. The power of blockchain that engulfs tamper-proof, verifiability, security can be employed to get rid of these things and prevent the attackers from modifying the log and forging fake identity cards. Blockchain technology can replace traditional systems with a highly trusted mechanism of managing digital identities.This paper proposes a distributed application for creation and issuance of identities on the blockchain network.

II. LITERATURE REVIEW

[1] implements a decentralized Dapp or distributed application for sharing objects on which users must have their own control on their documents. [2] proposes creation of blockchain-based decentralized application which can be used by students for application of transcripts, which can only be approved and issued by the intended institute, and by the Universities for the verification of the transcripts issued.[3] proposed blockchain based credential securing and verification system developed in ethereum test network.[4] proposed an architecture for biometric electronic identification document(e-ID) system based on blockchain for citizens identity verification in transactions corresponding to the notary, registration etc.[5] is a novel electronic identity document model, which uses a blockchain network combined with biometric authentication technology that can potentially solve several security problems.[6] developed a private permissioned blockchain network where individual's official documents can be shared by government bodies, organizations and educational institutes.[7] a mobile application that utilizes blockchain technology to create a secure protocol for storing encrypted personal information, as well as sharing verifiable claims about personal information.[8] proposed a system that can store identity information in ciphertext form and is jointly verified and maintained by the entire network node, thus it can guarantee the security and reliability of identity data in the digital identity authentication.[9] focuses on various aspects of blockchain technology like ethereum platform, smart contracts, ganache server, truffle framework, metamask, zero knowledge proof(ZKP) and also the implementation of development of sovereign identity using blockchain.

III. PROPOSED SYSTEM

CryptoID is a Dapp for issuing IDs on blockchain networks(Ethereum or Hyperledger), which will be verifiable and tamper-proof, for institutes or organizations.

The system functions include:

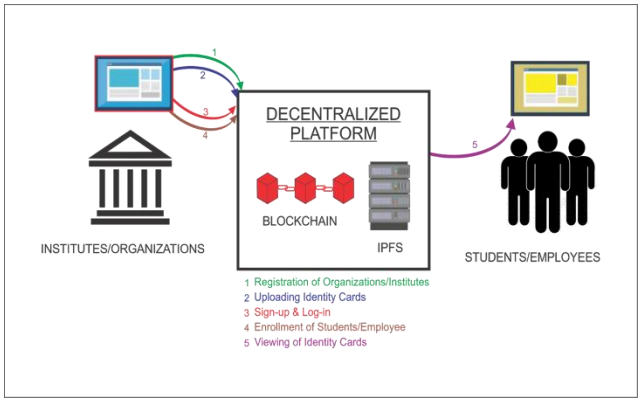
- Login for institutes/organization
- Registration of institute/organization
- Enrolment of students/employees

- Issuing/uploading of identity cards by institute/organization
- Retrieving/Verifying identity cards of individuals.

The system features include:

- Tamper-proof
- Verifiable
- Secure
- Decentralized

IV. SYSTEM ARCHITECTURE



V. SYSTEM WORKFLOW

- Registration of the Institute on Dapp.
- Registered Institutes with metamask will be able to issue the IDs of students/employees on the blockchain network.
- Fill the details of the candidate and the image file of ID.

The hash of the image file will be stored on blockchain and the image file will be stored on the Interplanetary File System(IPFS) which is a decentralized file storage system.

- The Institute can then create a website for the verification of candidates, showing their ID and details on the website through the Dapp.

Thus issuing of IDs on blockchain using Dapp will be done by the authorized identity of the Institute or Organization. The candidate can submit the id number to the website and the image of ID will be displayed with details on the Institute website or third-party website. The issuing of the IDs will be done on Dapp and not on the verification portal.

VI. PSEUDOCODE OF SMART CONTRACT

```
Registration of institute :
struct institute{
      address instituteAddress;
      bytes32 instituteName;
uintstudentCount;
mapping(uint => string) student;
   }
function registerInstitute(string memory _instituteName) public {
instituteCount++;
      institutes[msg.sender].instituteAddress = msg.sender;
      institutes[msg.sender].instituteName = hash(_instituteName);
   }
To store IPFS hash of image of identity card :
function newIdentityCard(uintenrollmentNumber,string memory ipfsHash,string memory _instituteName) public onlyRegisteredInstitute(_instituteName){
      institutes[msg.sender].studentCount++;
      institutes[msg.sender].student[enrollmentNumber] = ipfsHash;
   }
To retrieve hash of image of identity card :
function getIdentityCard(uintenrollmentNumber, address instituteAddress) public view returns(string memory){

return(institutes[instituteAddress].student[enrollmentNumber]);
   }
```

CONCLUSION

Our system ensures that the IDs generated are secure and reliable by implementing the blockchain using Dapp. There is no chance of ID duplication since issuance of IDs is done on Dapp and not on the verification portal. We have designed the secure and tamper-proof ID generation for Institutes and Organizations which involves human resources in their processes.AlsoIDs will be stored in decentralized formon IPFS platform. IDs are an integral part of the system that helps manage these resources in various aspects of the Institute and Organization and in their smooth functioning.

FUTURE ENHANCEMENTS

In the future we ought to enhance privacy, security and use it in different applications like issuing PAN cards/ Aadhaar cards or any other government /private authorities issuing identity cards on private or consortium blockchain platform.

REFERENCES

[1]. Chavan B. Amrita, Dr. Rajeshwari K, “The Design and development of decentralized digilocker using blockchain”,International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN(P): 2249-6831; ISSN€:2249-7493, Vol., Issue 2, Dec 2019, 29-36

[2]. Khedkar S., Powar A., Powar N., KilleChethan, KansaraH.,”TranscriptsDApp- A blockchain-based solution for transcript application”,

[3]. Rama Reddy T., Rayudu S., Raghavendra Ch V, Lalitha R V S, AnnupamaB.,”Proposing a reliable method of securing and verifying the credentials of graduates through blockchain”, DOI: https://doi.org/10.21203/rs.3.rs-45633/v1

[4]. Paez R., Perez M., Ramirez G.,Montes J.,Bouvarel L., “An architecture for Biometric Electronic Identification Document System based on Blockchain”,Future Internet 2020, 12; doi 10.3390/fi12010010

[5]. Juan D.M., PinerosR.A.,Paez R., Gustavo E.R.," A model for National Electronic Identity Document and Authentication Mechanism based on Blockchain", International Journal of Modeling and Optimization 8(3):160-165; doi:10.7763/IJMO.2018.V8
[6]. Malik G., Parasrampuria K., Reddy P. S., Shah S.,"Blockchain based identity verification model",Published in: 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)
[7]. TakemiyaM.,VanieievB.,"SoraIdentity:Secure, Digital Identity on the Blockchain",Published in: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)
[8]. Zhao G.,Di B., He H.,"Design and Implementation of the Digital Education Transaction Subject Two-factor Identity Authentication System Based on Blockchain",Published in: 2020 22nd International Conference on Advanced Communication Technology (ICACT)
[9]. Chavan A., Rajeswari K.,,"Design and Development of Self-sovereign Identity Using Ethereum Blockchain",International Conference on Sustainable Communication Networks and Application ICSCN 2019: Sustainable Communication Networks and Application pp 523-531