Identity Management using Blockchain Technology

Neer Chanchad[1], Darshan Limbani[2], Jude Silveira[3], Harsh Singh[4],Ms.Prajyoti Dsilva[5]

[1]IT Dept, SFIT Mumbai,India,neerchanchad2000@student.sfit.ac.in
[2]IT Dept, SFIT Mumbai,India,limbanidarshan2000@student.sfit.ac.in
[3]IT Dept, SFIT Mumbai,India, judesilveira1@student.sfit.ac.in
[4]IT Dept, SFIT Mumbai,India,hardharsho312@student.sfit.ac.in
[5]Professor, Dept. of Information Technology Engineering, St. Francis Institute of Technology(SFIT), Maharashtra, India

---***---

Abstract - *Identity Management involves the identification and authentication of a user to access the services provided by various sectors such as banking, healthcare, government, and online transactions. It also helps us set the level of access and authorizations a client has over a system. A few traits of traditional Identity Management Systems are they are insecure and fragmented. Thus the Identity Management System leveraging the Blockchain technology would enable safer management and storage of digital identities by providing unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises and users. In this paper, we propose the use of blockchain technology which is based on Ethereum to store the hash of identities on a blockchain. The hash of data is generated by the InterPlanetary File System (IPFS) and the corresponding hash is stored on the blockchain. The third-party is allowed to request documents from the user for identity verification, the user is then notified of the type of document being requested. The user can either share or deny access to the document. The outcome will be greater privacy, control of sensitive data, and faster access to services.*

Key Words: **Blockchain; IPFS; Ethereum; Privacy; Hashing; Identity Management;**

1. INTRODUCTION

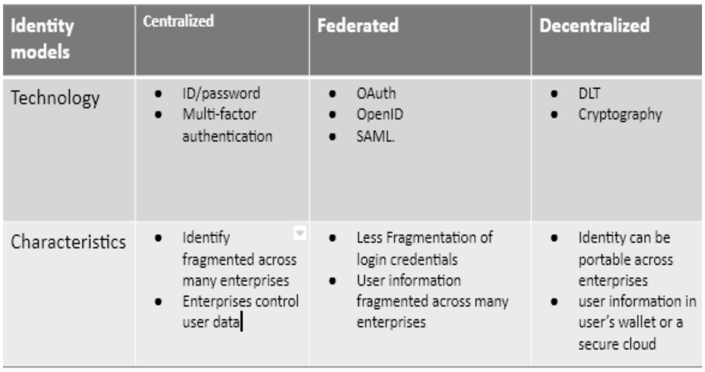
Data leaks or identity fraud (e.g., stealing of credentials or credit card in- conformation) frequently affect profitable loss and drop of trust in the identity providers. Within this environment, new identity operation results that satisfy the factual requirements must be explored. The particular data is traditionally stored in a centralized system, which makes it possible for hackers or bushwhackers to achieve their vicious pretensions by robbery/ misusing/ manipulating these data in this centralized system [1].

To gain access to the services handed by these online operations, the customers must validate their identity by giving a valid identifier. This identifier can take numerous forms similar to particular information contained on a social security card, automobile license, passport, birth certification, and academy or work badges. Identity Management is the process of authenticating, authorizing, and identifying a thing (individually or a group of people or the system) to access one or further many resources. The biggest point of the blockchain is its decentralization where the whole database is maintained by all the bumps on the network. An agreement medium ensures that the creation and modification of data are agreed upon by all the bumps or the maturity of the bumps. Using this fashion the blockchain has the features of high security, not easy to be tampered with, and so on

2. RELATED WORK

Identity management systems authenticate, authorize and identify users. Many private institutes or government organizations need personal information from users to provide them with the required services. Traditionally this information is stored in centralized databases. Centralized databases are prone to data breaches and the users had minimal or no control over their information. The lack of transparency causes privacy issues in the identity verification process. With the emergence of Bitcoin, blockchain technology has started entering all the areas of global business. With its strong features such as distributed ledger, immutability, and transparency, blockchain technology is a new approach to identity management systems. Due to decentralization, the users have more control over their identity and there is no centralized authority.

Table-1: Study on different Identity Models



Identity models	Centralized	Federated	Decentralized
Technology	• ID/password • Multi-factor authentication	• OAuth • OpenID • SAML.	• DLT • Cryptography
Characteristics	• Identify fragmented across many enterprises • Enterprises control user data	• Less Fragmentation of login credentials • User information fragmented across many enterprises	• Identity can be portable across enterprises • user information in user's wallet or a secure cloud

In here, we briefly go through some of the technologies mostly used in this domain:

Ethereum: It is an open-source blockchain platform that supports smart contracts functionality. It is a network of several nodes which are used to transfer money or store data. Each machine runs an Ethereum client. There is only one main Ethereum network and many test networks. Ether is a cryptocurrency used for paying gas, which is nothing but an operational cost of the transaction. Application-based on Ethereum is usually referred to as Decentralized Application or Dapp.

Smart contracts: They are lines of code, which define a set of rules that control the transfer of assets and manage agreement between users. It has three properties: code, data storage, and balance of ether owned by the account. The execution of smart contracts charges transaction fees in ether, which depend on the processing power required. Once the smart contract is deployed it cannot be altered, making transactions secure from unwanted modifications.

Solidity: It is a JavaScript-based language used to write Smart Contracts for Ethereum networks. It is intended to center around Ethereum Virtual Machine (EVM). Solidity supports features like inheritance, import of libraries. It uses .sol extension and it has strict typing rules at compile time.

Web3.js: It is an Ethereum based JavaScript Application Programming Interface(API). It is used to interact with the remote or local Ethereum network using HTTP or IPC connection from JavaScript applications.

Metamask: It is a chrome extension used to interact with the Ethereum network. It turns a normal browser into an Ethereum browser enabling websites to retrieve data from the blockchain and letting users securely manage identities and sign in. It can also be used to store the data. One user can create many accounts and all the accounts are encrypted and securely stored within your browser .

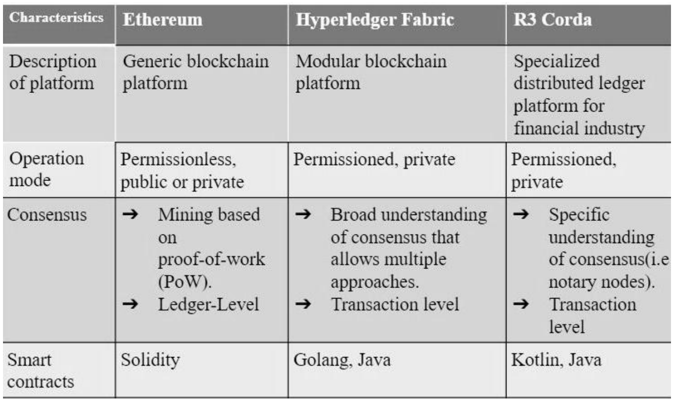
IPFS: InterPlanetary File System (IPFS) is a decentralized database built on top of MongoDB. With a peer-to-peer implementation, it avoids a single point of failure and protects data from denial of service attacks.

Truffle:

Truffle is a world-class development environment, testing framework, and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier.

Truffle supports developers across the full lifecycle of their projects, whether they are looking to build on Ethereum, Hyperledger, Quorum, or one of an ever-growing list of other supported platforms. Paired with Ganache, a personal blockchain, and Moralis which is a leading web development platform that offers everything that the user needs to create, host, and grow great dApps in one place along with the full Truffle suite of tools promises to be an end-to-end app development platform.

Table -2: Comparison of different blockchain technologies



Characteristics	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	Generic blockchain platform	Modular blockchain platform	Specialized distributed ledger platform for financial industry
Operation mode	Permissionless, public or private	Permissioned, private	Permissioned, private
Consensus	➔ Mining based on proof-of-work (PoW). ➔ Ledger-Level	➔ Broad understanding of consensus that allows multiple approaches. ➔ Transaction level	➔ Specific understanding of consensus(i.e notary nodes). ➔ Transaction level
Smart contracts	Solidity	Golang, Java	Kotlin, Java

3. ARCHITECTURE

A decentralized and distributed or a blockchain network consists of nodes that are organized together to store, share, update and keep track of blockchains (sometimes also called ledger or digital transaction data). The nodes of the blockchain network may include computing devices or systems such as PCs, laptops, servers, computer farms or clusters, virtual or cloud systems, smartphones, or tablets.

The nodes may keep a partial or an exact copy of the blockchain which may help to verify/audit existing transactions or transactions that may happen in the future by validating the hash values of transaction blocks.

Adding a new block to the blockchain may need the consensus of the blockchain network and the consensus protocol/scheme must make sure that every new block that is added to the Blockchain is the only version of the fact that is accepted upon by all the nodes in the Blockchain[2].

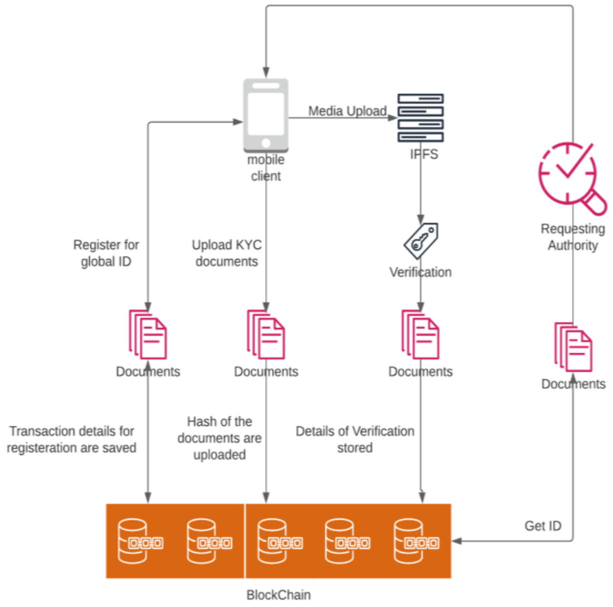


Fig -1: System Architecture

In the proposed system, the users can add their identity on a blockchain through our web-based application which acts as an interface among users, third parties, and the database. The user can either register with the help of an existing Ethereum account via Metamask or create an account on the system and then link an Ethereum account to the system to successfully register the user.

After successful registration, the user can upload his/her details and identity through the web application. The transaction gets created which can be signed by the user with the help of Metamask to post it to the blockchain.

When the third-party requests access to the user data, the appeal is sent to the concerned user. The user can view the demand and see what details have been requested by the requesting party as well as the public address of the requesting authority. On the user's approval, the generated hash would be sent to the requesting party. The user can then give partial access or complete access to his/her credential through our web app. After the user updates the access to the credential, the requesting party can then view all the fields of the uploaded credential approved by the user.

Manipulation of a database is thus prevented by the Blockchain Database architecture as changing any minute detail in the Block's data means that the Hash of that Block is changed and since it is connected to every subsequent Block in the chain, the Hash of each following Block alters. This means that the Miner has to Mine every Block again and travel all the blocks collectively to the network.

4. PROPOSED WORK

In this system, users can sign-up to the system by entering the required details. Installation of Metamask is a must for the user since it helps in signing transactions and linking the Ethereum wallet to the account.

Then to access his account the user has to enter the login credentials. After the authentication is successful, the user will be directed to his respective homepage.

The account offers the following functionalities to the user:

1)Uploading Documents:

The user can upload his documents to the portal. Once uploaded the documents are stored in the IPFS and the generated Hash is then stored on the user's blockchain address.

2)Granting Access to Documents:

After successful verification of the uploaded documents. The requesting authorities can then request details from the uploaded documents. Once the request is received by the user. He can either accept it and grant the necessary information or reject it. Also, User has an option to provide partial access to the asked information.

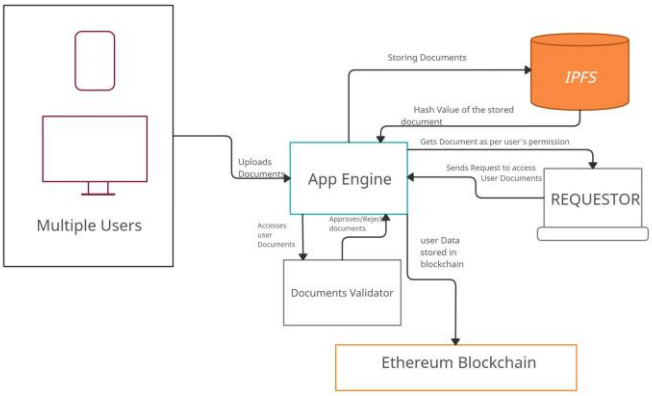
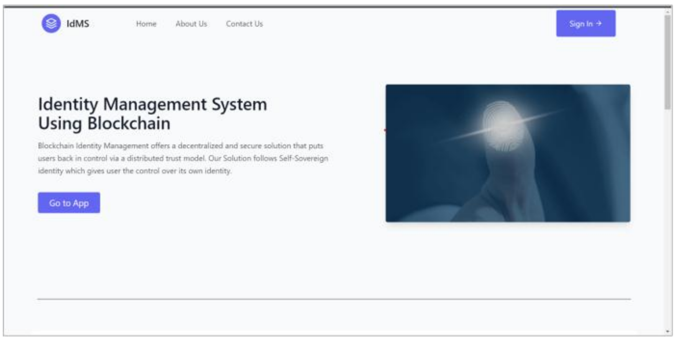

Multiple Users
Uploads Documents
App Engine
Storing Documents
IPFS
Hash Value of the stored document
Gets Document as per user's permission
Sends Request to access User Documents
REQUESTOR
Accesses user Documents
Approves/Reject documents
user Data stored in blockchain
Documents Validator
Ethereum Blockchain

Fig -2: System Design[3]

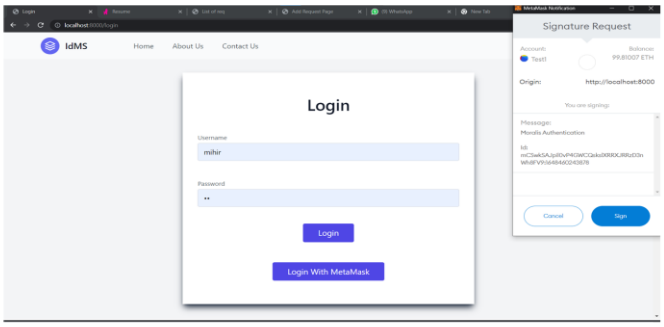
5. IMPLEMENTATION



Identity Management System Using Blockchain

Blockchain Identity Management offers a decentralized and secure solution that puts users back in control via a distributed trust model. Our Solution follows Self-Sovereign identity which gives user the control over its own identity.

Fig -3: Home Page :User Side



Login

Username: mihir

Password: ••

Account: Test1

Balance: 99.81007 ETH

Origin: http://localhost:8000

You are signing:

Message: Moralis Authentication

Id: mCSwkSAJpl0vP4GWCQskslXRRXJRRzD3nWh8FV9:1648460243878

Fig -4: Login Page : User Side

After clicking on the 'Go to App' or Sign up button (as shown in Fig.)the user will be redirected to the login page where he has the option to login through credentials or using MetaMask

(a browser extension for accessing ethereum wallet).

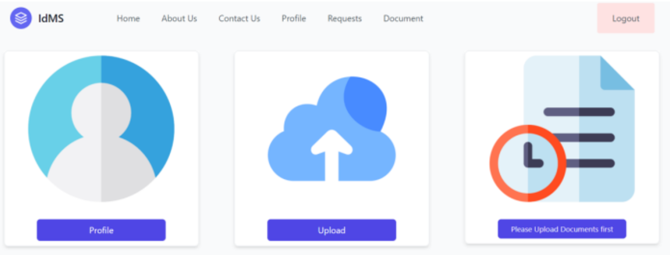
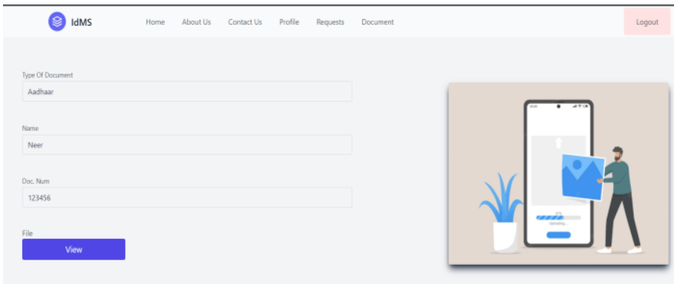


Fig -5:Dashboard Page : User Side



Type Of Document: Aadhaar

Name: Neer

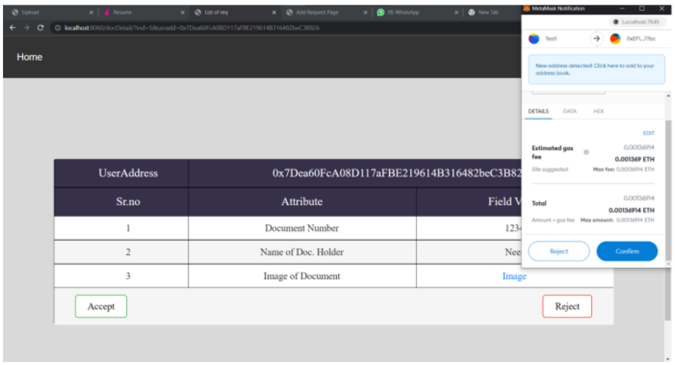
Doc. Num: 123456

File

Fig -6:Upload Page: User Side

In the Profile Section the user can edit specific information if necessary--Although it is important for the user to add ethereum address in order to make data transactions

(i.e upload or change documents).



localhost:8060/docDetail/?ind=5&usradd=0x7Dea60FcA08D117aFBE219614B316482beC3B826

UserAddress	0x7Dea60FcA08D117aFBE219614B316482beC3B82	
Sr.no	Attribute	Field V
1	Document Number	123
2	Name of Doc. Holder	Nee
3	Image of Document	Image

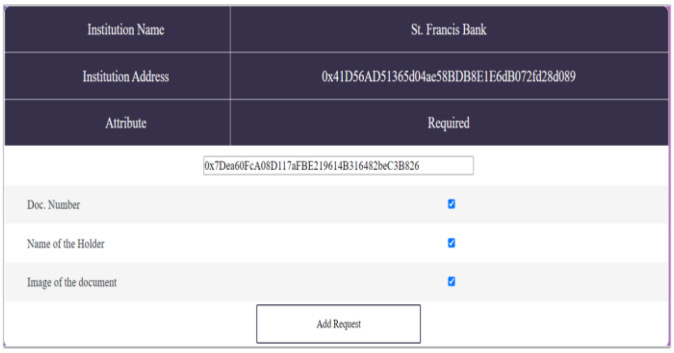
New address detected! Click here to add to your address book.

Estimated gas fee: 0.00136914 — 0.001369 ETH — Site suggested — Max fee: 0.00136914 ETH

Total: 0.00136914 — 0.00136914 ETH — Amount + gas fee — Max amount: 0.00136914 ETH

Fig -7:Verification page : Verifying Authority

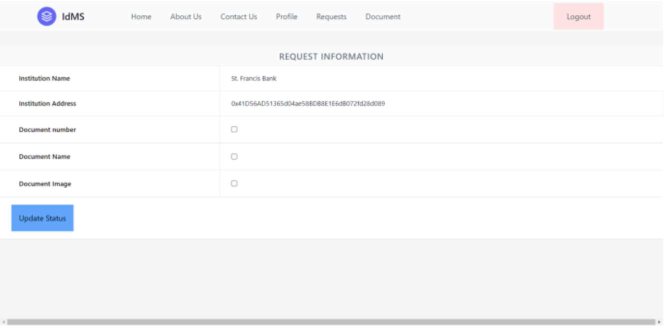
The Verification Authority verifies the document uploaded by the user and decides whether the documents are valid or not and signs the transaction with the help of Metamask browser extension.



Institution Name	St. Francis Bank
Institution Address	0x41D56AD51365d04ae58BDB8E1E6dB072fd28d089
Attribute	Required
	0x7Dea60FcA08D117aFBE219614B316482beC3B826
Doc. Number	☑
Name of the Holder	☑
Image of the document	☑

Fig -8:Requesting Authority Page

The concerned Administration in-charge can request a variety of identification documents from the users after the documents are verified.

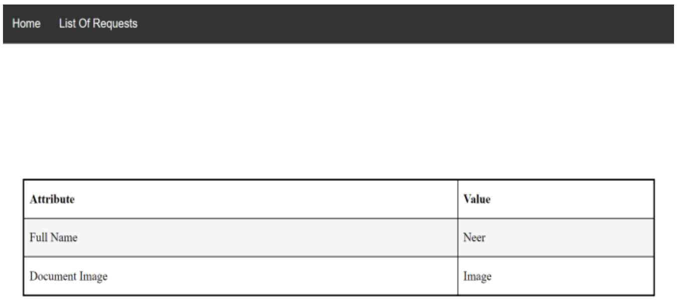


REQUEST INFORMATION

Institution Name	St. Francis Bank
Institution Address	0x41D56AD51365d04ae58BDB8E1E6dB072fd28d089
Document number	□
Document Name	□
Document Image	□

Fig -9:Request Detail:User Side

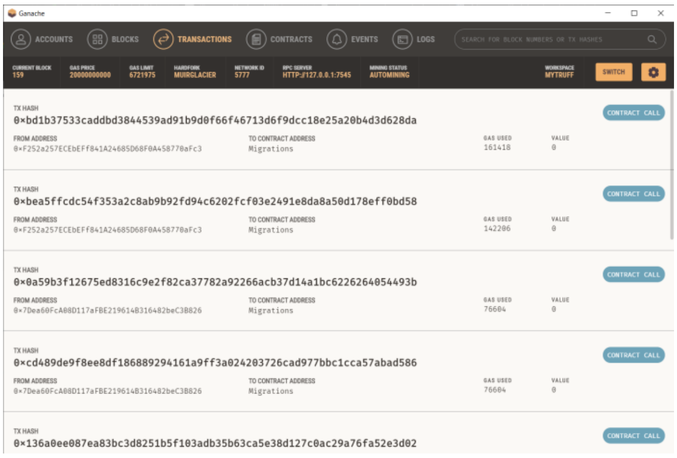
The third part of the user dashboard allows users to act upon the requests sent by the institution. After being directed to the list of request pages the user can take the desired actions.



Attribute	Value
Full Name	Neer
Document Image	Image

Fig -10:View Request Page

The above image is again the part of institution side interface where the institution can access the attributes to which the user gave access.



```
CURRENT BLOCK  GAS PRICE    GAS LIMIT  HARDFORK     NETWORK ID  RPC SERVER              MINING STATUS  WORKSPACE
159            20000000000  6721975    MUIRGLACIER  5777        HTTP://127.0.0.1:7545   AUTOMINING     MYTRUFF

TX HASH
0×bd1b37533caddbd3844539ad91b9d0f66f46713d6f9dcc18e25a20b4d3d628da
FROM ADDRESS                                  TO CONTRACT ADDRESS    GAS USED   VALUE
0×F252a257ECEbEFf841A24685D68F0A458770aFc3    Migrations             161418     0

TX HASH
0×bea5ffcdc54f353a2c8ab9b92fd94c6202fcf03e2491e8da8a50d178eff0bd58
FROM ADDRESS                                  TO CONTRACT ADDRESS    GAS USED   VALUE
0×F252a257ECEbEFf841A24685D68F0A458770aFc3    Migrations             142206     0

TX HASH
0×0a59b3f12675ed8316c9e2f82ca37782a92266acb37d14a1bc6226264054493b
FROM ADDRESS                                  TO CONTRACT ADDRESS    GAS USED   VALUE
0×7Dea60FcA08D117aFBE219614B316482beC3B826    Migrations             76604      0

TX HASH
0×cd489de9f8ee8df186889294161a9ff3a024203726cad977bbc1cca57abad586
FROM ADDRESS                                  TO CONTRACT ADDRESS    GAS USED   VALUE
0×7Dea60FcA08D117aFBE219614B316482beC3B826    Migrations             76604      0

TX HASH
0×136a0ee087ea83bc3d8251b5f103adb35b63ca5e38d127c0ac29a76fa52e3d02
```

Fig -11:Blockchain Transactions

This image of the Ganache-- Local Blockchain server--shows the transactions of the blockchain. This part is only accessed by System Administrator.

6. CONCLUSIONS

Our Project demonstrates how blockchain technology can be applied to identity management for improving security. The image of the document gets stored on the IPFS and the hash of this document along with the other details entered by the user gets stored on the blockchain. Any third party can request the data from the user by mentioning the user's public address and the user has the right to approve, reject or partially approve the document request. These transactions also get stored on the blockchain.

REFERENCES

[1] Komal Gilani, Emmanuel Bertin, Julien Hatin, Noel Crespi,“A survey on blockchain-based identity management and decentralized privacy for per-sonal data”. BRAIN 2020: 2nd conference on Blockchain Research Ap-plications for Innovative Networks and Services, Sep 2020.

[2] Faber, Benedict, Georg Cappelen Michelet, Niklas Weidmann, RaghavaRao Mukkamala, and Ravi Vatrapu. ”BPDIMS: A blockchain-based per-sonal data and identity management system.” In Proceedings of the 52ndHawaii International Conference on System Sciences. 2019.

[3] El Haddouti, Samia, and M. Dafir Ech-Cherif El Kettani. ”Analysis of identity management systems using blockchain technology.” In 2019 In-ternational Conference on Advanced Communication Technologies andNetworking (CommNet), pp. 1-7. IEEE, 2019.

[4] Alsayed Kassem, Jamila, Sarwar Sayeed, Hector Marco-Gisbert, ZeeshanPervez, and Keshav Dahal. ”DNS-IdM: A blockchain identity manage-ment system to secure personal data sharing in a network.” Applied Sci-ences 9, no. 15 (2019): 2953.

[5] https://www.leewayhertz.com/blockchain-identity-management/