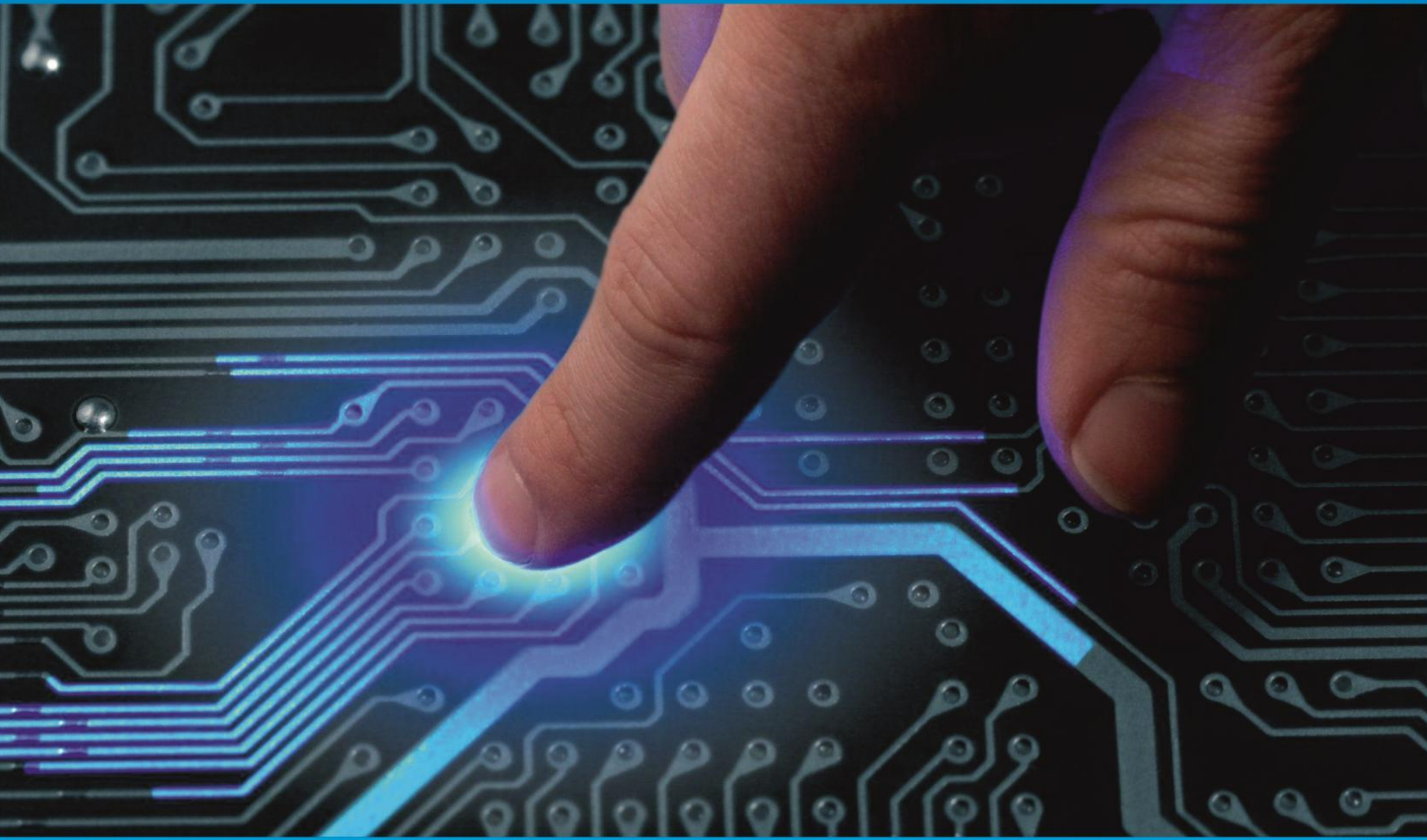
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904108 |

Blockchain Based Identity Management System

Shresht Choubey[1], Hardik Vora[2], Viraj Shah[3], Ms Smita Bansod[4]

BE Student, Dept. of I.T., Shah & Anchor Kutchhi Engineering College, Mumbai University, India[1,2,3]

Assistant Professor, Dept. of I.T., Shah & Anchor Kutchhi Engineering College, Mumbai University, India[4]

ABSTRACT: The blockchain innovation is profiting a few enterprises with straightforwardness, security and a lot more highlights, increasing the value of their organizations. Therefore, it is to be accepted that it is good to go to change the present working too, in a profoundly secure manner. The existing framework of an identity management system is neither secure nor solid. At each point, you are being approached to recognize yourself through various government-approved IDs like Voter ID, Passport, Pan Card thus on. Sharing numerous IDs prompts protection concerns and information breaks. Consequently, the blockchain can clear the way to self-sovereign personality through decentralized networks. A self-sovereign character guarantees protection and trust, where character records are made sure about, confirmed and supported by permissioned members.

I. INTRODUCTION

Individuals share their own data online by techniques for various cloud sources or advantage associations that can put their ID records into an ignoble hand. Also, online applications keep up concentrated servers for dealing with information; it gets less hard for programming specialists to hack the servers and take the delicate information. While joining on different online stages, clients need to make a novel username and riddle word each time. It gets hard for a fundamental individual a blend of a username and secret key for getting to various services. Maintaining indisputable endorsement profiles is a real testing task. The current affirmation process consolidates three assistants, including attesting affiliations/KYC affiliations, clients, and untouchables that need tocheck the character of the client. The general structure is extravagant for all these stakeholders. Since KYC affiliationsneed to serve mentioning of various parts, for example, banks, restorative organizations suppliers, movement pros, require more points of interest to process their necessities quickly. Therefore, KYC affiliations need to charge a higher sum for the check which is passed to people as took care of dealing with costs.
Utilizing blockchain for the character the board can permit people to have obligation regarding character by making a general ID to fill different prerequisites.

A few empowering late headways in development have convinced various fans to acknowledge that we are at the forefront of a mechanical progression that can be used to comprehend a Self-Sovereign Identity Management System. With the happening to blockchain advancement, many acknowledge that such development can give the specific foundation whereupon the possibility of self-sovereign character can be made sense of it. This has fuelled the vitality where many use-cases for different circumstances are being explored to grasp the sensibility of such a structure. Regardless of the way that such examination is fundamental to drive the bleeding edge, one unexpected indication is that there exist different thoughts about what the term self-sovereign character suggests.

In this following paper, we will try to introduce a new data model to eliminate the existing traditional identity management systems and overcoming its drawbacks.
The new model will consist of a combination of blockchain and identity management which enables decentralized identity storage which results in avoiding a central authentication authority and prevents interference with the store data and identities.

II. LITERATURE SURVEY

Blockchain is basically an open, decentralized and an immutable ledger that can store transaction or information of any kind in a hashed manner. The data is stored collectively in the form of blocks[11]. The first block – also known as the genesis block – consists of only data and the hash value of the data. The next block will consist the data, the hash value of the genesis block, as well as the actual hash value of the data present in it. The third block will contain the data of its own, along with its hash value and the hash value of the second block. They are connected in that way in form of a chain and hence the coined term – Blockchain.[11] The immutability of the Blockchain can be observed in a very simplistic way. If somebody tries to tamper with the actual data in the block, the concurrent hash value of that data would change drastically and will no longer match with the hash value present in the next consecutive block. Since this ledger is distributed to every node / person in the network, the copies with everyone else will reflect the actual data and this manipulation of the data will be ignored.[6][11][10]

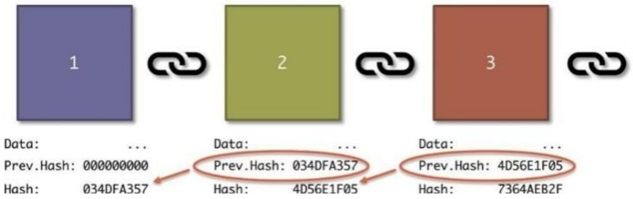
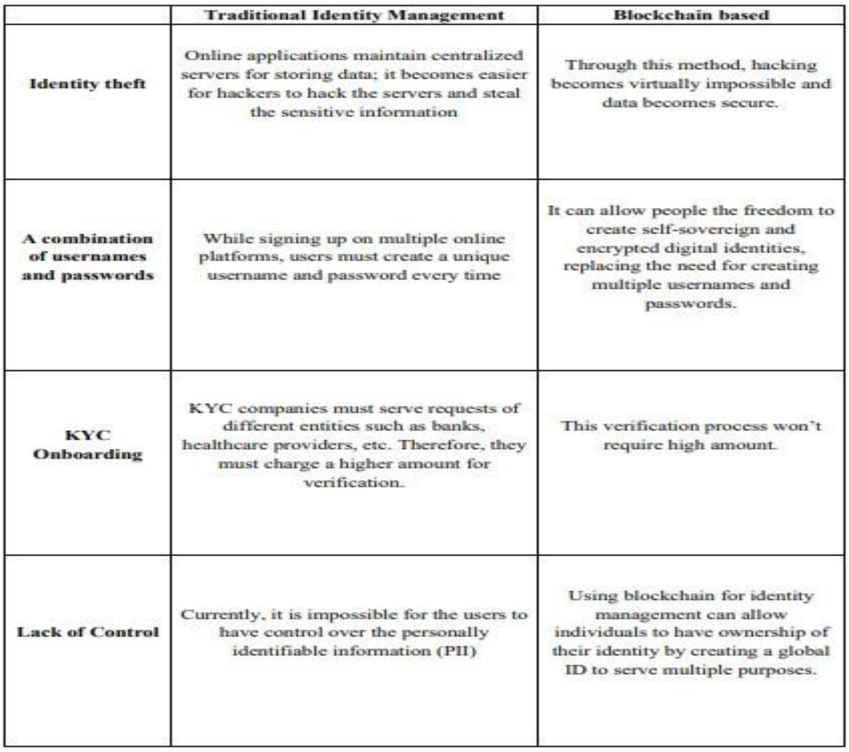


Figure 1: Basic blockchain

Individuals identify themselves using various identity assets such as their name, national identity number and passport number. Identity assets are recorded in physical identity documents which are attested by central authorities.[6] Apply for a loan, open a bank account, buy a sim card, or book a ticket, use of identity documents can be the cases in which it is used. Companies such as government institutes, banks, credit agencies are the weakest point in the current identity management system. As a matter of the fact, it has become crucial to move away from intermediary and provider-controlled identity management models toward user-
controlled digital identity.[3][5]



	Traditional Identity Management	Blockchain based
Identity theft	Online applications maintain centralized servers for storing data; it becomes easier for hackers to hack the servers and steal the sensitive information	Through this method, hacking becomes virtually impossible and data becomes secure.
A combination of usernames and passwords	While signing up on multiple online platforms, users must create a unique username and password every time	It can allow people the freedom to create self-sovereign and encrypted digital identities, replacing the need for creating multiple usernames and passwords.
KYC Onboarding	KYC companies must serve requests of different entities such as banks, healthcare providers, etc. Therefore, they must charge a higher amount for verification.	This verification process won't require high amount.
Lack of Control	Currently, it is impossible for the users to have control over the personally identifiable information (PII)	Using blockchain for identity management can allow individuals to have ownership of their identity by creating a global ID to serve multiple purposes.

III. PROPOSED SYSTEM

An individual will first have to register on website to establish his/her identity. After registering, a user profile will be generated with a digital wallet account on MetaMask. The wallet would be used to store the Ethers that are necessary to pay for the transactions on the blockchain. Once the account on the wallet is established, it will generate a unique ID that would help to identify the user while requesting the documents and during verification of the authenticity and identity of the transaction user. In our case, the identification document that we are going to use is a driver's licence. After the customer gets unique ID number, they need to move the association gave IDs on the application which will be saved in the IPFS having hashed addresses managed in the blockchain. The application will expel the individual information from these ID's; so, customer can do self-validation of his/her details.

Initially, the user enters his credentials to create an account. The account gets linked to the Meta Mask wallet which can be used to conduct various transactions. The address of the account is a 64-bit hash. The user can then add the driving license details which are hashed together and stored in a blockchain on the network. The image file of the driving license is stored on the IPFS on the network.

The institute can then request the data from the user by identifying the user using the same 64-bit unique ID. After requesting access to the information, the user can grant access to the institution. The user chooses which information to display from the requested queries. After the user grants request, it reflects in the institution data that the user has granted access to the information. If the user grants access to the license file, it is retrieved from the IPFS. The information can be viewed by the institute. The displaying of information solely works based on consent provided by the user.

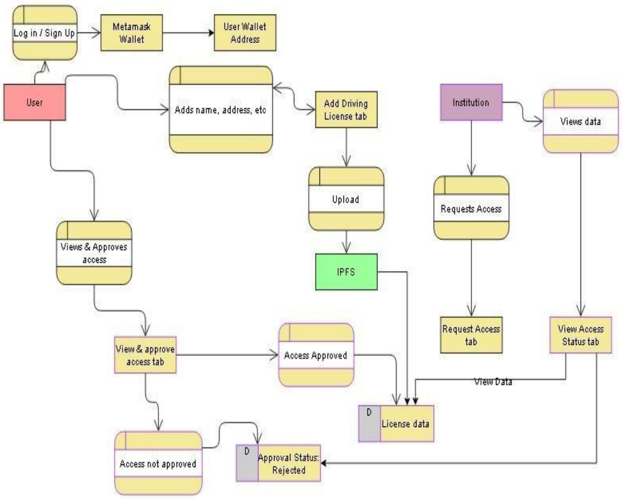


Figure 2: Workflow diagram

IV. IMPLEMENTATION

What would such a system provide?

- **Unique global ID:** Each user who registers on Blockchain identity management system will get a unique identity number. User's unique ID number consists of all personally identifiable information in an encrypted format that is stored on their device backed by IPFS. Users can simply share unique ID with any third-party to authenticate themselves directly through the Blockchain Identity Management

- **Consent:** A blockchain identity management system will not store any user's information. Moreover, the system uses Smart contracts to enable the controlled data disclosure. No transaction of user's information can occur without explicit consent of the users.

- **Decentralization:** No personal identification documents of the users will be stored in a centralized server. All the documents that identify users get stored on their device backed by IPFS, making it safe from mass data breaches.

  Using the Blockchain identity management backed by IPFS doesn't allow any hacker to steal the identifiable information.

➢**A universal ecosystem**: The blockchain identity management doesn't set to any geographical boundaries. So, users can use the platform across the borders to verify their identity.

User Interface:

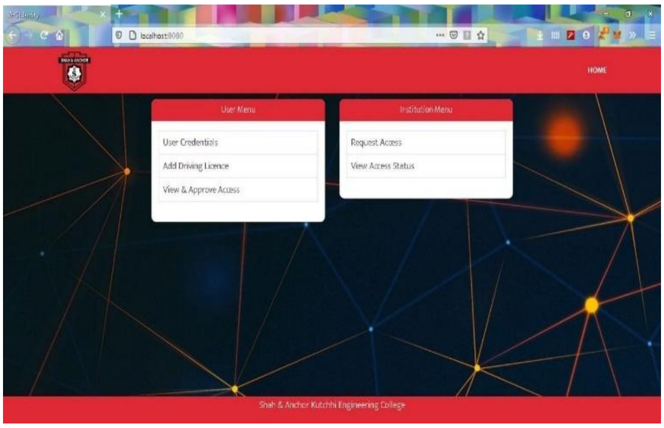


Figure 3: Home Page

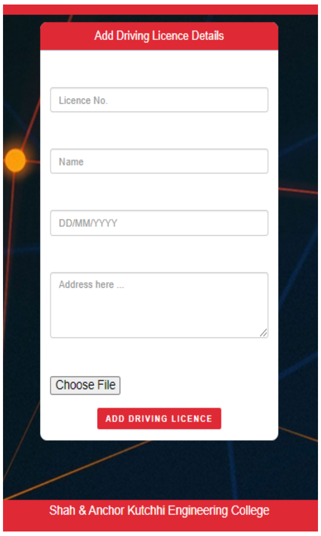
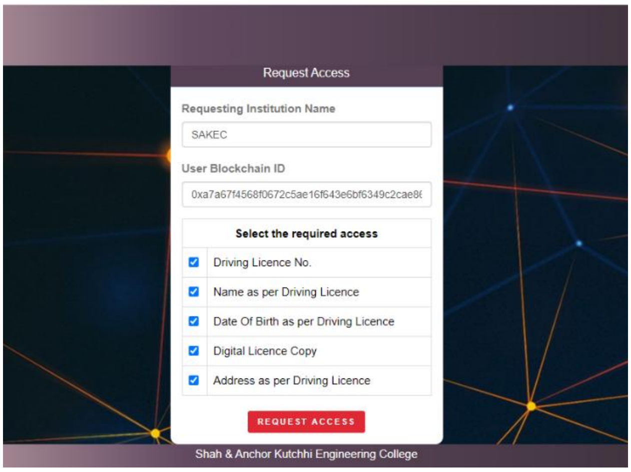


Figure 4: Adding driving license of the user


Request Access

Requesting Institution Name

SAKEC

User Blockchain ID

0xa7a67f4568f0672c5ae16f643e6bf6349c2cae8

Select the required access

☑ Driving Licence No.

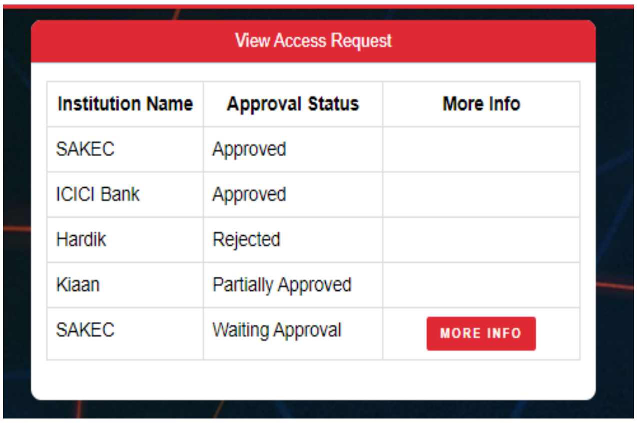
☑ Name as per Driving Licence

☑ Date Of Birth as per Driving Licence

☑ Digital Licence Copy

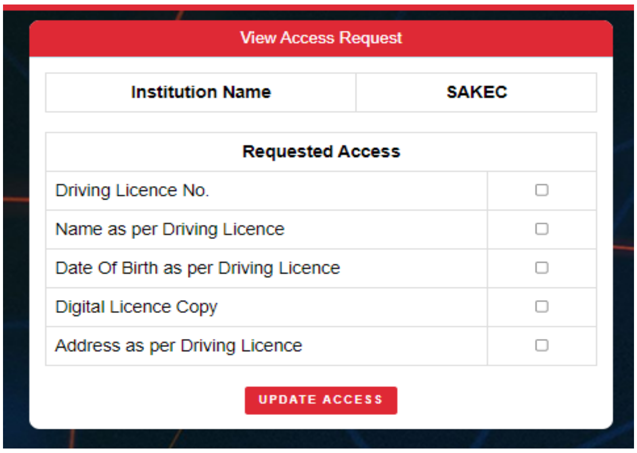
☑ Address as per Driving Licence

Figure 5: The information about the user's identification can be requested.



View Access Request

Institution Name	Approval Status	More Info
SAKEC	Approved	
ICICI Bank	Approved	
Hardik	Rejected	
Kiaan	Partially Approved	
SAKEC	Waiting Approval	MORE INFO



View Access Request

Institution Name	SAKEC

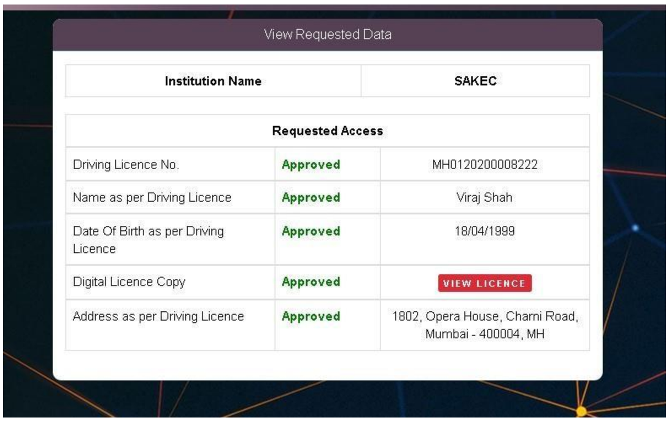
Requested Access	
Driving Licence No.	□
Name as per Driving Licence	□
Date Of Birth as per Driving Licence	□
Digital Licence Copy	□
Address as per Driving Licence	□

Figure 6.1 & 6.2: The request from institution appears and by clicking on “MORE INFO’, the user can choose which information to grant access to.

As shown in the above test case, for every transaction performed, be it adding the data in the chain, or requesting a certain information from an individual and also granting access, a certain value must be paid to add the data into the network. Since the network is public, the authenticity of the transaction can be verified. As shown in the user’s section, the user can choose to display the information according to the need and convenience. And when approved, the institution can view which information is partially approved, or completely approved or just rejected. The data is visible in the text form and the license uploaded is visible in the image form retrieved from the IPFS. Every transaction conducted generates a unique hash which is obtained after payment. The transaction details along with the time stamp can either be viewed in the Metamask wallet or on the test network’s ledger of transactions.

The transactions were conducted over the Rinkeby Testnet which is one of several Ethereum Testnet which offers basically the same functionalities that the Ethereum Mainnet provides, but for a currency that is freely attainable. After every transaction, a separate page is designed to display the hash that can be used to verify that the transaction is successful from the test network block explorer. The transaction details are also stored permanently in the MetaMask wallet for further checks.

To place the transaction in the blockchain, it roughly takes 15 seconds as that is the specified time for the block to be created in the Rinkeby Testnet. Ethers to conduct the transaction can be easily obtained from the Rinkeby
The “Approved” status says that all the requested data was made available to the institution. The “Rejected” status means that the request of the institution was denied. The “Partially Approved” status means that only some of the requested data of made available to the institution faucet for free. The gas price is a small mandatory fee for the transaction which is a very small percentage of 1 unit of that Ether.



View Requested Data

Institution Name	SAKEC

Requested Access		
Driving Licence No.	Approved	MH0120200008222
Name as per Driving Licence	Approved	Viraj Shah
Date Of Birth as per Driving Licence	Approved	18/04/1999
Digital Licence Copy	Approved	VIEW LICENCE
Address as per Driving Licence	Approved	1802, Opera House, Charni Road, Mumbai - 400004, MH

Figure 7: The institute can view the data as granted by the user

V.CONCLUSION

In conclusion, building of such a prototype would help to understand the scope and basic mechanism of an already existing Identity Management System when implemented on a distributed system. The implications of such a system would be reflected in the test case scenarios. With the technology that comes in hand with Blockchain, it can be safely assumed that the version of the system that would be developed would offer functionality far superior than the normal existing systems. The innovative nature of such a technology brings transparency and a sense of trust in the ecosystem by its very nature of decentralization and with the efficient processing due to the smart contracts.

Having this form of control not only eases out the process of exchanging documents with the institution, but also eliminates any chances of forged exchanges. The approval of the user works like a self-attested form of a document which can only be done by the user and is easier to keep track of.

The future scope of this project would be to establish more components of uploading and requesting identification documents as a driver’s license simply is not enough in most of the processes. Documents like Voter’s ID, a PAN Card, Aadhar, Passport would be very close to a complete digital identification setup. Requesting and Granting access would become as easy as a click of a button but in a more secure and sovereign way. The user holds all the authority in sharing of these documents. It could also revolve around just one unique digital currency that does not have a very high market value but just enough to not undermine the system and have some credibility.

REFERENCES

[1] Wie Liang Sim, Hui Na Chua, Mohammad Tahir, Blockchain for Identity Management: The Implications toPersonal Data Protection, 2019 IEEE Conference on Application, Information and Network Security (AINS).

[2] Arshad Jamal, Mariam – Aisha Fatima, Blockchain – Based Identity Verification System, 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET).

[3] Quinten Stokkink, Johan Pouwelse, Deployment of a Blockchain based Self – Sovereign Identity, 2018 IEEE Conference.

[4] Mehmet Aydar, Serkan Ayvaz, Towards a Blockchain based digital identity verification, record attestation and record sharing system, June 2019.

[5] Samia El Haddouti, M. Dafir Ech-Cherif El Kettani, Analysis of Identity Management Systems Using Blockchain Technology.

[6] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In 2015 IEEE Security and Privacy Workshops. San Jose, CA: IEEE.

[7] Do, H., & Ng, W. (2017). Blockchain-based System for Secure Data Storage with Private Keyword Search. 2017 IEEE 13Th World Congress on Services.

[8] Yasin, A., & Liu, L. (2016). An Online Identity and Smart Contract Management System. In 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). Atlanta, GA: IEEE.

[9] Soliman, A., Bahri, L., Carminati, B., Ferrari, E., & Girdzijauskas, S. (2015). DIVa: Decentralized identity validation for social networks. In 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). Paris: IEEE.

[10]Md Sadek Ferdous, Farida Chowdhury and Madini O. Alassafi. In search of self – sovereign identity leveraging Blockchain Technology. IEEE.

[11]S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (2008).

[12]Reza Soltani, Uyen Trang Nguyen and Aijun - An. Practical Key Recovery Model For SelfSovereign Identity Based Digital Wallets 2019 IEEE International conference on cyber science and technology congress.

[13]Crompton, M., & McKenzie, R. (2010). Current Issues and Solutions in Identity Management. 32nd International Conference Of Data Protection And Privacy Commission.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING