Digital Identity Management System Using Blockchain

Sulochana Devi
Department of Information Technology
Xavier Institute of Engineering
Mumbai, India
sulochana.d@xavier.ac.in

Shrineeth Kotian
Department of Information Technology
Xavier Institute of Engineering
Mumbai, India
shrineeth.kotian@gmail.com

Manish Kumavat
Department of Information Technology
Xavier Institute of Engineering
Mumbai, India
manishkumawat12955@gmail.com

Dixit Patel
Department of Information Technology
Xavier Institute of Engineering
Mumbai, India
dixitpatel902015@gmail.com

***Abstract*—Digital Identity Management is a new identity management model in which the holder of the identity data really have the ownership of their own identity data and have full access control over it without involving any intervenor. This has created in huge amount of user information with the service providers, resulting in two difficulties, user owned private data is saved and left to the care of such third party applications and the user does not have ownership of his own data. Maintenance of such multiple identities will only become more difficult as the digital era unfolds. We attempt to solve this problem by using the Blockchain technology for digital identities. Blockchain is an enabling technology for building Digital Identity that offers a decentralized and secure environment. A blockchain's data is cryptographically connected and distributed across multiple computers, making them nearly impossible to temper with. Hence, Blockchain technology is the best and the secured platform to build Digital Identity. The existing system of identity management is neither secure nor reliable. Therefore, the blockchain can create a path to Digital Identity through decentralized networks, which will assure privacy, trust and security.**

Keywords*—*Blockchain, Self-sovereign Identity, authentication mechanism, Identity management, verification.

I. INTRODUCTION

An identity of an individual or an organisation can be represented using a set of attributes association with the entity such as name, address, etc. Identity management includes maintaining the data used for identity and their access control. A Holder, an Issuer, and a Verifier are the three key actors in the Identity management system.

The identity issuer, a trusted party such as local government, can issue personal credentials for an identity holder (a legal individual / organisation). By issuing any user's data, the identity issuer attests to the validity of the personal information in that credential. The last name and date of birth, for example. The identity holder can store those credentials in their personality identity wallet and use them later to prove statements about his or her identity to a third party, the verifier of the identity data. An identity attribute is a piece of information about an identity, and a credential is a collection of many identity attributes (a name, an age, a date of birth). A credential is a verifiable claim, which includes some facts that is attested and digitally signed by the issuer about the holder. Credentials are issued by third parties who vouch for the accuracy of the information included inside the credential. A credential's usefulness and dependability are totally dependent on the issuer's reputation and trustworthiness. The fact in a credential can be the holder's identity data (For example, D.O.B) or other types of factual data (e.g. a GPA). Anyone (for example, an employer) can be a claim verifier after establishing a trust relationship with the issuer. The verifier requests a specific credential (for example, a person's birth certificate) and checks the authenticity of the credential using the issuer's signature.

Identity management is challenging if holders do not have a full control over their identity data, since the data are usually maintained at third-party issuers' sites i.e. Government institutes, Banks, and Credit agencies which are considered the weakest point in the current identity management system as they are vulnerable to theft and hacking of data. Thus, the blockchain comes with the possibility of eliminating intermediaries while allowing citizens to manage identity independently. The concept of digital identity allows holders to retain ownership of their identities and control over how their identity data is used.

II. LITERATURE REVIEW

Individuals can identify themselves using various identity documents such as their name, national identity number and passport number, etc. The traditional methods of identity management are open and susceptible to data breaches, identity theft and frauds can also occur. A solution to this is blockchain, where blockchain enables identity owners to have control over their identity and identity based personal documents, control access to their records i.e. they can manage to whom they share their details and for what purpose their data is used, and allows identity owners to share minimum amount of information while totally ensuring integrity and trust. This particular study focuses on things such as using the Blockchain technology for identity sovereignty purpose. The paper contains the followings which explains current problems in traditional identity management methods, and then tells about Blockchain technology, explains why the technology fits for a digital identity management system, and the concepts that are used in Blockchain based identity management systems. There were many problems in the traditional system which included problems like privacy, security, usability, globalization, etc. Blockchain is basically a distributed ledger which is immutable by anyone, which stores the ownership of digital documents in the form of transactions and blocks. In this, the asset owners are identified by an asymmetric cryptographic i.e. public-key cryptography which means the user's public key, It uses asymmetric cryptography concept in order to assign digital identity to the documents added. [1]

Digital identity is basically the digital representation of the information known about some specific individual or sometimes an organization. It can be defined as a distinguishing character or a personality of an individual which makes him stand apart from a crowd of people. This identity of an individual can be stolen, which is termed as Identity Theft, which is in turn defined as usage of someone's credentials like personal information credentials without that particular person knowing about it and using it for other purposes mainly fraud. The main idea behind verification of a user is that it will require additional identity information for example, mother's name can be used as a proof to qualify to be the owner of the documents that are stored like credit card or pan card or any other documents. This two factor authentication can be carried out with the help of the zero knowledge proof method, which is basically a method mostly a mathematical method which is used to verify an individual without even sharing or revealing any of their data. [2]

The functional view of the system consists of the registration process where identity record will be uploaded and stored and then its usage. There is a way to detect duplicacy of documents which consists of putting the strong identifiers in a hash table and look for collisions to occur, and it should be a distributed hash table. The advantages of this system include that the actual values of the registered documents used as proofs for multi-factor authentication and privacy is provided security using ZKP. There is an assurance that the information provided is totally valid. It allows a flexible approach to authentication and a validation approach to information. Thus, Identity Management and Theft Protection are major areas of concern and active work which is drastically growing. This Identity Management system has potential to provide an environment which is secure and collaborative by providing a solution to the problem of Identity Theft with the help of privacy preserving multi- factor authentication. [2]

In this system we saw the benefits of blockchain in digital identity management. The challenges like identity theft, kyc and the major problems of the IDs and passwords that can be easily solved by it. Uploading the documents on decentralised servers which is backed up by IPFS. And using Blockchain identity management backed up by IPFS doesn't allow any hacker to steal the personal information of the user and mainly without the consent of the user no third party can get the access of the user's data. [3]

In today's world identity management plays a very important role for getting any of our work done. Whether a small scale or a large scale company everyone needs to show their identity. But in our existing system everywhere we have to submit the copies of our data and many more. It is possible the submitted data can be manipulated. So there rises a risk in identifying the right data and to verify all this it would consume much time and money. This technique is neither reliable nor secure. Blockchain Identity Management offers a complete reliable and secure environment for everyone around the world. Keeping the ID's and documents on a decentralized application and can be used whenever necessary. This technology will help to keep our important data safe and allows us to share the data only to the consent person. All the transactions made are clearly visible to all the users thereby giving a trust to the users of their confidential data and will make the path easier for all the users. [4]

Blockchain based identity management is a powerful and uses decentralized method for storing data and keeping the records of a transaction for every user. Blockchain is a secure and reliable method for keeping the transactions securely. It is very much indeed to use such technologies because in the current system, the confidential data which we submit to the third party can even leak our data. There are many cases of data leaks nowadays and this shared data can even be used by frauds in illegal ways. Digital Identity management keeps a track with whom we share our documents and confidentials. [4]

In this paper, the authors proposes a conceptual design and high-level architecture for a Blockchain-based Personal Data and Identity Management System (BPDIMS), a human-centric and GDPR-compliant personal data and identity management system based on blockchain technology. In this paper, they have discussed about the concept of MyData which was published by the Finnish government. MyData facilitates the idea that users should have a better idea of where their data is stored, who uses it, and be able to change this. It is a humanistic approach to people's data and aimed at giving full control over the personal data back to users. The main objectives of the MyData from the user perspective are right to know what personal information exists, right to see the content of personal information, right to rectify false personal information, right to audit who accesses personal information and why, right to obtain their personal information and access it freely, right to share/sell personal information to others., and right to remove or delete personal information. [5]

The key stakeholders in the proposed system, BPDIMS are User : end users, utilizing the system, Service provider : company providing a service to user, either paid or free, Data purchaser : an entity (company or person) purchasing the user data for a specific stated purpose, Data validators : entities who validate the user data to check that it belongs to that particular user or not. The system consists of several components, namely three blockchain layers which is basically smart contract blockchain, access blockchain and identity blockchain, Off chain data that particular user or not. The system consists of several components, namely three blockchain layers which is basically smart contract blockchain, access blockchain and identity blockchain, Off chain data that particular user or not. The system onsists

of several components, namely three blockchain layers which is basically smart contract blockchain, access blockchain and identity blockchain, Off chain data that particular user or not. The system consists of several components, namely three blockchain layers which is basically smart contract blockchain, access blockchain and identity blockchain, Off chain data Here encryption proposed are symmetric-key algorithms like Rijndael AES, Diffie- Hellman key exchange algorithm or even public key infrastructure. Lastly, the User interface to give an overview over all personal data of the user and to be able to manage all the data and system functionalities. In our system consent appears in three ways : Consent for processing personal data in return for services, Consent for storing personal data, and Consent for selling/access to personal data. All user's consent are stored on the Access Blockchain of the system. The second and third type of consent regarding monetization and storage is linked to the Smart Contract Blockchain. [5] Then the paper depicts the benefits of this blockchain based user-centric personal data management system in detail. The system is benefited with all the secured features of blockchain technology, trusted and fully-automated self- enacting smart contract technology, implementation of storing data using various secured encryption and hashing methods i.e. cryptography. [5]

In this paper, the authors propose a scheme to implement Privacy Enhanced Digital Identity with CP-ABE. Although Digital Identity ensures traditional security such as data integrity and secure access to data, the data protection of electronic documents has yet to be regulated. According to the authors, encryption based on ciphertext policy attributes (CP-ABE) can improve data protection. In Digital Identity, documents of subscribers are hosted on public cloud which is assumed to be a trusted entity. However, cloud storage can be unreliable and prone to insider attack. CP-ABE (Ciphertext Policy Attribute-Based Encryption) is a newer cryptographic mechanism that can improve data protection. However, correct implementation and efficiency are still a major concern for the overall implementation. Attribute- based encryption (ABE) is the encryption method in which the encryption is carried out under a number of attributes. ABE is classified in Key-Policy ABE (KP-ABE) and CP- ABE. In KP-ABE, the access policy is encoded in the subscriber's private key and a number of attributes are encoded in the ciphertext. In CP-ABE, the access policy is encoded in ciphertext and a number of attributes are encoded in the subscriber's private key. In CP-ABE, the recipient can only decrypt the ciphertext if the set of required attributes encoded in the recipient's private key meets the access guidelines encoded in the received ciphertext. Finally, the scheme proposed to prepone part of the encryption process to increase performance. This preponed process creates a token which can be reused later. The proposed system has been shown to be safe and secure against IND-sAtt-CPA games. According to the authors, the proposed scheme can be further improved by using homomorphic encryption that enables encrypted computing and post-quantum ABE schemes to be used for both, although schemes exist, but they are not yet trivial or practical. [6]

Digital Identity is basically a digital document wallet where you can store your documents. It is used to store documents such as government issued documents, academic certificates, etc., so that the documents can be shared easily on the web or wherever it is required. It provides access to the user to their stored documents for various public and private purposes. As it is a software made by the government and as a key initiative of the Digital India program, there was a beta version of Digital Identity launched. It basically works around Aadhar card number. But there are always security reasons related to Aadhaar card number and One Time Password generated which provides access to Digital Identity stored documents. There have been many such cases where OTPs has also been illegally accessed and as of Aadhaar card numbers, they would be more easily known . [7]

The problems with the traditional system was that a citizen of India need to show their personal documents everywhere before they can enjoy privileges to avail any kind of services depending upon the services they want to avail. In some cases it might happen that the required documents might not be physically present at that time. The documents required can be anything ranging from personal identity card to any personal or academic documents or important documents. There has been many such cases where it has been experienced by many people they were not able to present the required document at that required moment of time. The problems that exists in the traditional systems can be broadly enlisted as the document is not properly verified so proper verification or the authenticity of the documents by government agencies can cause difficulties, there may be difficulties faced during submission of multiple copies of the physical documents periodically and there maybe very high chances that the original documents can be lost or stolen or the chances of the original documents being damaged due to wear and tear from usage since a long long time. [7]

There are some benefits of Aadhaar linked Digital Identity too. Digital Identity holds two types of certificates, one of which is educational and the second one is lifetime. There is an alert one month prior to the expiry date to some documents such as a driving license or a passport, and it may prompt to change it or update it and upload an updated document. The process being very transparent, once it gets logically linked with UIDAI and then PAN card, it can then verify more accurately by matching the uniqueness of the user's first name, parent's name or guidance's name but at the same time last name can be failure. There have been many security disadvantages of the system which includes the key security concerns of authentication, authorization at client-server, both end and secure communication at the time of data traversal. Any data transfer should be done in

an encrypted form with high level of encryption standards, and there should be a maintenance of data integrity, and verification of trust between both parties and exchange of trust certificates so that trust should be maintained. [7]

III. PROPOSED WORK

A. Identity management approach:

Identity management is a process to create and maintain a user account to be used for authentication and to identify in online services. It is required to simplify the user provision process and to make sure the rightful users can have access to the services. The Identity management system cycle comprises of four phases including enrolment, authentication, issuance and verification.

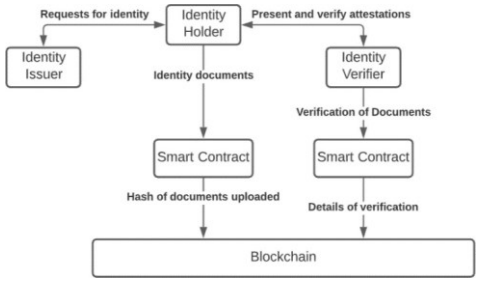

Fig. 1. Overview of Digital Identity Management

In digital identity, owners of identity are central to the management of the identities, to make it possible that they are able to administer their personal credentials on personal mobile devices or cloud.

The Digital Identity management provides the ownership of data to the user to promote full user control and transparency is also achieved. Based on rules of need-to-know and need- to-retain, the owner of the data can control the personal information without relying on third parties that can result in data lost or any misuse of sensitive personal information resulting in the security of the information.

B. Blockchain:

A Blockchain is basically a database that runs a software that is used to validate and then it shares new entries with all the participants.

It is essentially a distributed ledger of records, across nodes. These records are maintained in blocks. Each new block has to be mined by data miners by solving a complex problem. Every block references to its preceding block. This blockchain is registered across all its nodes, and that is the reason why blockchain is called immutable. It would take a great computing power to hack a blockchain, distributed across multiple nodes. Hence, data on a blockchain cannot be changed. Blockchain is the major principal of Bitcoin transactions. Thus, blockchain provides the following functionalities:

1. Decentralized distribution

2. Immutable

3.Security

4. Transparency

5. Authenticity

C. Methodology:

Firstly we have the web application in which the user sign ups by entering basic details like name and email using his/her metamask address. This information would then be stored in the blockchain. System does not store any user's private identity data on blockchain.

Whenever user wants to use some services then firstly user share his/her identity to the verifier for verification. Verifier checks the shared identity, verify the identity and authenticate the user and allow the user to use servives. This event gets stored as consent proof of data sharing i.e. transaction details happened between the identity owners and the verifying parties with time stamps.

Between all this transaction we will implement Smart Contracts which omits the need for a third party in each and every transaction. Smart Contracts increase the level of trust and security from both sides at reduced costs and also requires less time, as the conditions are stored in blockchain and executed through immutable program code. The access management is based on this Smart Contracts, so that it enforced time limits for the access of the user's data to the verifier. After the time limits over, the consent is revoked automatically from the verifying party.

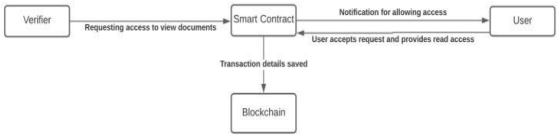

Fig. 2. Working of Digital Identity System

IV. RESULTS

We have made a smart contract to store the hash of the documents or credentials that the user submits in the server and which gets stored in the IPFS Server. Smart contracts are basically simple programs which gets stored on a blockchain. These programs are meant to run when specific conditions are met, here the condition is when the user submits the documents in IPFS.

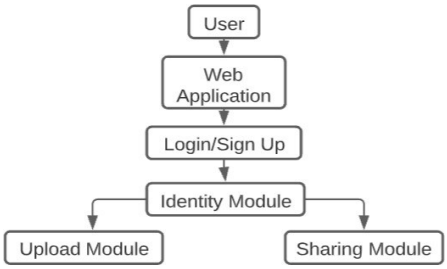

Fig. 3. Overall Flow of User Activity

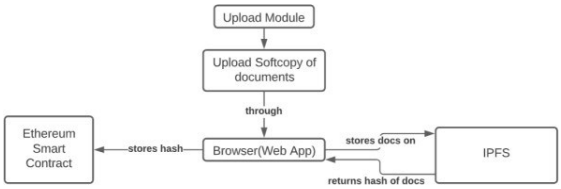

Fig. 4. Flow of Upload Module

Here is the module after the user will enter his details and click on the Identity tab in the user module. Firstly, he will have to connect his Metamask wallet to the blockchain server. Once the wallet has been successfully connected, the user gets directed to the user module.

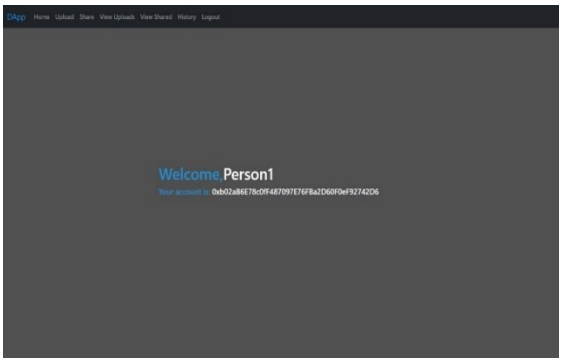

Fig. 5. User Dashboard

After logging in this is the first page user visits, where the user's name and his/her metamask public address will be displayed. And there are many options available for the user such as upload identities, share identities, view uploaded and shared identities, and history of all past transactions.

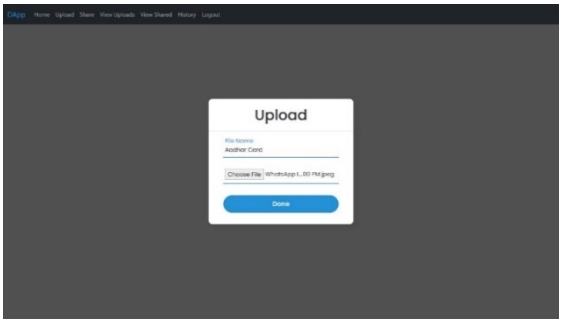

Fig. 6. Upload Module

This is the upload module wherein user uploads their identities. User needs to give name of the credential that is being uploaded and choose that credential and click on done button.

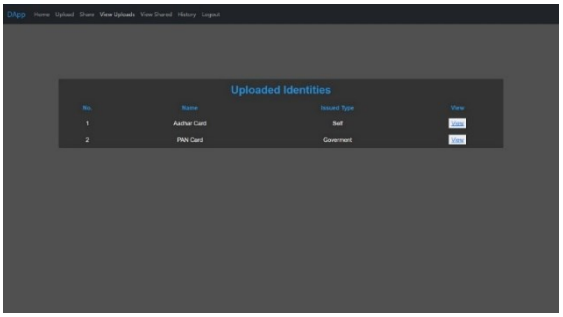

Fig. 7. View Uploads Module

This is the view uploads module where user views all their uploaded identities.

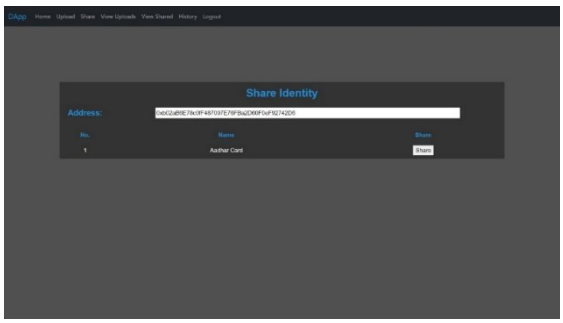

Fig. 8. Share Identities Module

When the user wants to share their identity, this is the place where the user needs to come and enters the metamask public address of the person to whom the user wants to share an identity.

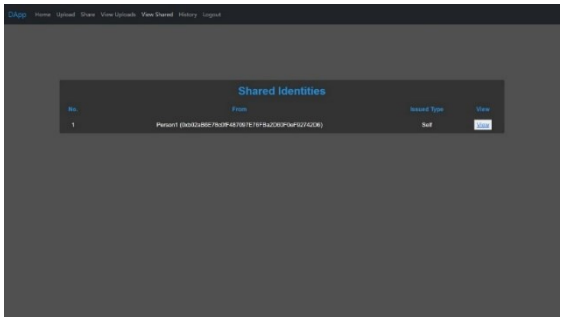

Fig. 9. View Shared Module

This is the view shared module where user views all the identities shared to him/her.

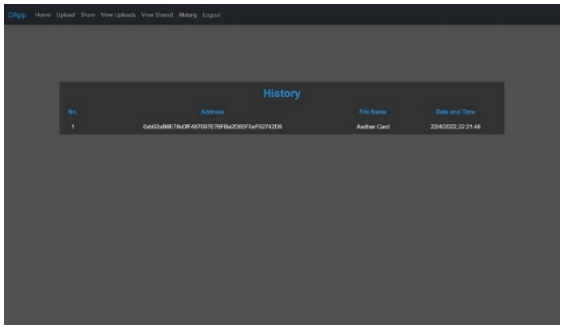

Fig. 10. Transaction History

In this module, user can view their transaction history of shared identities with date and time.

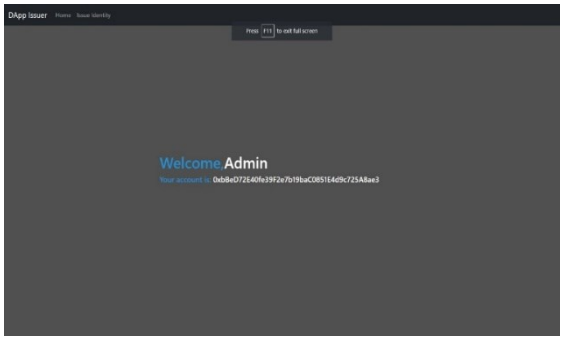

Fig. 11. Admin Module

This is the Admin module, which can be only accessible by the admin of the system.

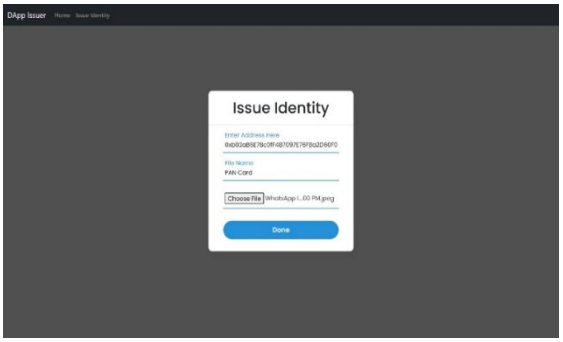

Fig. 12. Admin's Issue Identity Module

This is the issue identity module which is only accessible to admin. Here, Admin can issue identity to the user.

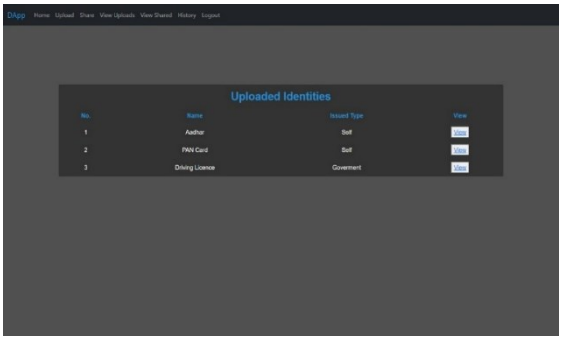

Fig. 13. View Issued Identities Type

This is the view uploads module where the user views all their uploaded identities. In this, the user can view the issued type of the identity i.e. Self-issued (user themself had uploaded the identity) and Government issued (these are the identities that had been issued by the admin).

V. CONCLUSION

Thus we have planned on laying a foundation for a decentralized digital identity using Blockchain as Self-sovereign identity, including modern cryptography and verifiable digital credentials. We enlisted the problems and challenges that exists in the traditional identity management methods in terms of security, privacy, usability and globalization. We reviewed existing solutions in the literature, and proposed a blockchain system which leverages features of Blockchain to realize a protected, private, secure and globally usable digital identity system, in which identity owners have full control over their portable stored identity in the form of documents and identity based records or files. For future work, we intend to explore possibilities of integrating our solution on mobile applications, and try making it totally secured and make it usable to every range of age group and by any nation with ease.

REFERENCES

[1] Mehmet Aydar, Serkan Ayvaz and Salih Cemil Cetin, "Towards a Blockchain based digital identity verification," Towards a Blockchain based digital identity verification, vol. 1, no. Digital identity verification, p. 22, (2020).

[2] E. Bertino, "Digital Identity Management Techniques and Policies," p. 31, (2019).

[3] A. Takyar, "Blockchain Identity Management: Enabling Control Over Identity," LeewayHertz - Software Development Company, (2021). [Online]. Available: https://www.leewayhertz.com/blockchain-identity-management/.

[4] L. X. G. T. B. P. N. D. L. C. W. S. Zhimin Gao, "Blockchain-based Identity Management with Mobile Device," (2018).

[5] G. M. N. W. R. R. M. R. V. Benedict Faber, "BPDIMS:A Blockchain-based Personal Data and Identity Management System," (2019).

[6] S. N. Puneet Bakshi, "Privacy Enhanced Digital Identity using Ciphertext-Policy Attribute-Based," (2020).

[7] D. V. Kumar, "A Solution to Secure Personal Data When Aadhaar is linked with Digital Identity," (2018).

[8] Y. L. H. Y. P. Q. L. Xiwei Xu, " Design Patterns for Blockchain-based Self -Sovereign Identity," (2020).

[9] https://www.youtube.com/watch?v=5Uj6uR3fp-U

[10] https://www.researchgate.net/profile/Nikita_Patil3

[11] https://patents.google.com/patent/US20060163344A1/

[12] https://tykn.tech/identity-management-blockchain//

[13] https://decentralized-id.com/companies/tykn-tech/

[14] https://www.youtube.com/watch?v=QQYjNOPneuA

[15] https://www.youtube.com/watch?v=6BVTIMzHOuc

[16] https://www.youtube.com/watch?v=_160oMzblY8

[17] https://blockchain.mit.edu/how-blockchain-works

[18] https://www.youtube.com/watch?v=SSo_EIwHSd4

[19] https://www.youtube.com/watch?v=X06TQOOBrhM

[20] https://www.youtube.com/watch?v=YVgfHZMFFFQ

[21]https://www.sciencedirect.com/science/article/pii/S1364032118307184

[22]https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

[23] https://etherscan.io/

[24] Xiaohui Yang, Wenjie Li , “A zero-knowledge-proof-based digital identity management scheme in blockchain,”(2020).

[25] https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf