IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111120

Identity Management System Using Blockchain

Prof. Pratibha Kashid (Guide)[1], Jadhav Akshada Kiran[2]

Department of Information Technology, Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India[1,2]

Abstract: Identity management solutions are generally designed to facilitate the management of digital identities and operations such as authentication, and have been widely used in real-world applications. In recent years, there have been attempts to introduce blockchain-based identity management solutions, which allow the user to take over control of his/her own identity (i.e. self-sovereign identity). In this paper, we provide an in-depth review of existing blockchain-based identity management papers a.

Keywords: Blockchain, digital identities, multi- factor authentication, cryptographic, Security.

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.

LITERATURE SURVEY

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. 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.

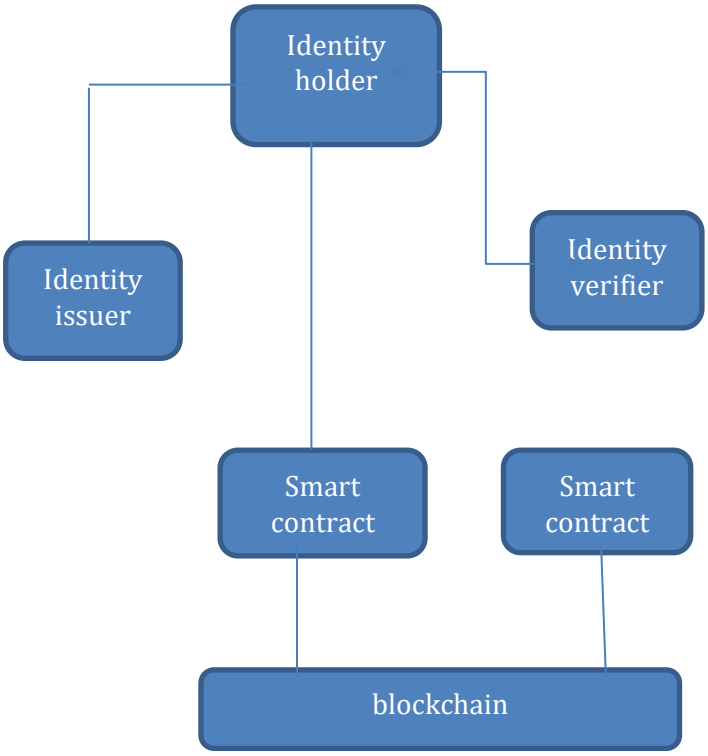
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022

DOI: 10.17148/IJARCCE.2022.111120

Sr.no	Year	Proposed Model	Limitations
1.	2019	Digital identity management system using blockchain	There are many problems in traditional management system.it consist of storage of data for short period of time
2.	10 nov ember 2020	Identity management system	Includes privacy ,security, usability globalization
3.	2020	Blockchain base identity mangment system	It includes the data can aslo haked very easily ,manintaning data is very difficult task to do so .



(a)Fig. overview of digital identity management

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.

SYSTEM OVERVIEW

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.

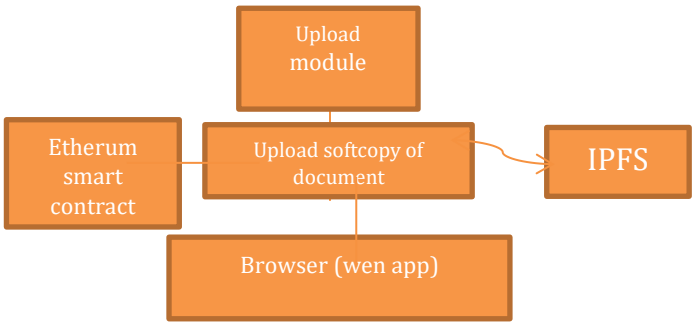
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111120

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-toknow 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.

(b) Fig. flow of upload module :



CONCLUSION

Thus we have planned on laying a foundation for a decentralized digital identity using Blockchain as Selfsovereign 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.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 11, November 2022
DOI: 10.17148/IJARCCE.2022.111120

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-identitymanagement/.
[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 Blockchainbased 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 Blockchainbased 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/S13640321183071
[22]https://journals.plos.org/plosone/article?id=10.1371/journal.pone.01 63477
[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