IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 6, June 2024

DOI: 10.17148/IARJSET.2024.11620

BLOCKCHAIN-BASED SOCIAL NETWORK USING USER'S IDENTITY MANAGEMENT

Varsha P Kumar[1], Siddarth HA[2], Lakshmi HK[3], Prasanna Kumar M[4]

Student, Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India[1]

Student, Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India[2]

Student, Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India[3]

Professor, Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, India[4]

Abstract: People's use of social networks is growing, but because of the centralized data management system They've got to deal with the issue of privacy leaks. This privacy issue is resolved by dispersed social network catered emergency services, but they introduce efficiencies in the provision of primary functionality such data availability and access control. According to this perspective, social networks and decentralized social networks face the aforementioned difficulties. To build a new decentralized social network architecture combining the advantages of decentralised networks and classic centralized social networks, we take advantage of the newly popular blockchain technology. We provide central control services using the blockchain, which functions as a trusted server. To ensure that users have total control over their data, we divide the storage services in the interim. Blockchain-based social network of user's identity management systems offer improved efficiency, and enhanced user experiences.

Keywords: Blockchain, decentralized system, privacy, security.

I. INTRODUCTION

Social networks are online platforms that enable individuals to connect with one another. It is a significant platform for people to talk about their lives, exchange opinions, and collect and distribute information. Due to the widespread usage of social networks, it is evident that connecting with them online is a highly favoured pastime among Internet users. These days, the majority of social networks are centralized, meaning that once users accept the terms of service set forth by social network firms, the companies frequently hold all user data. Nonetheless, a number of agreements grant online social network firms the authority to use user data for customized purposes. As a result, users even cease using these online social networks. All user data is uploaded to and stored on centralized servers under the supervision of online social network firms as a result of data and service centralization. As a result, users find it challenging to safeguard their social network material in the event that servers fail. To exacerbate the situation, user addresses and other security information, such as passwords, may be compromised if the servers are compromised. Credential stuffing attacks allow hackers to quickly breach the accounts of several people who use the same password on various websites. Users' private information is therefore vulnerable to theft and misuse. Researchers are encouraged to think about creating an online social network based on the decentralization framework because of these issues with centralized social networks. With more control of ownership information and privacy, decentralized social networks may provide consumers a safer and more manageable social network experience. The reliance on centralized servers for service has diminished due to the dispersed storage of data. Generally speaking, a peer-to-peer mechanism powers decentralized social networks, with each node supporting the service and storing a portion of the data. It does not, however, bind wicked deeds.

II. RELATED WORKS

Social network of user identities is a key issue facing the current world. Technological progress, in particular the introduction of 5G networks and Internet of Things IoT, has led to a significant increase in the number of entities on the digital landscape. In this way it is essential to digitally identify not only individuals, but also organisations, services, applications and devices in an efficient and appropriate manner. In order to meet these objectives, it has been proposed to manage user identities on social networks, although they are still at an early stage of development. To ensure the safe storage of customers' personal data, legacy identity management systems rely on a number of centralised organisations or reliable central business operators. [1] Describes the architecture and design for a blockchain-based human-centric personal data and identity management system called BPDIMS.

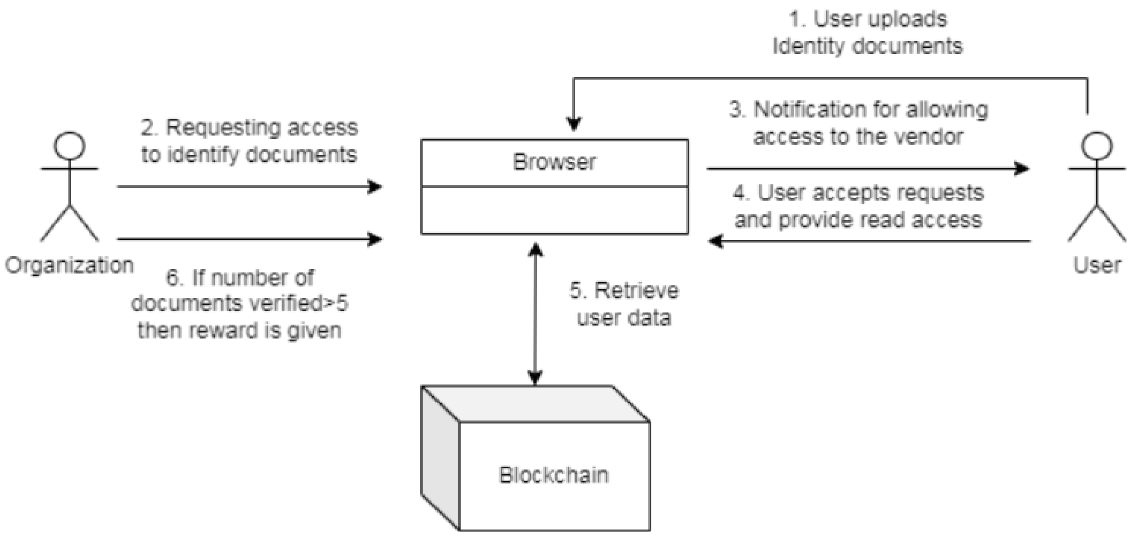
DOI: 10.17148/IARJSET.2024.11620

The system complies with GDPR regulations. They made use of the principle of "My Data," which supports the premise that customers ought to be allowed to modify where, who, and how their data is utilized. [2] Stated the necessary conditions for Self-Sovereign Identity (SSI) and its potential to safeguard digital identities, lower transactional risks for all involved, and enhance trust and privacy online. For the survey, they employed the two SSI canonical and reusable use cases, "Online Identity Verification" and "Discover, Connect, Create Credential." Their research validates that current blockchain-based SSI solutions outperform their non-blockchain equivalents. [3] Explains how consumers have made it standard practice to keep user accounts with many service providers in order to access a variety of services in today's digital environment. All identity-related characteristics need to be validated for the system to work properly; otherwise, the resources are open to data loss and financial risk. To ascertain current industry practices, a comparative analysis of these identity management systems was carried out. Furthermore, certain issues with the identity management systems of today have been noted. The article helps choose the Identity Management System that will work best for a certain application. [4] Gives a consistent understanding of the fundamental concepts of SSI for various SSI treatments, such as identity proofing and authentication techniques. It began with a summary of identity management strategies, looking at the architecture of the system and the key participants in it. It also discussed blockchain technology as a possible solution for distributed user-centric identification. Next, the methods for digital identity verification and authentication were examined. Finally, it elaborates on challenges, highlights knowledge gaps in the field, and outlines existing solutions. [5] Explains Identity management solutions are usually developed to facilitate the handling of digital IDs, and real-world applications often require procedures such as authentication. Recently, an attempt has been made to develop a system of identity management based on the blockchain that would allow individuals to manage their own identities autonomously. Highlighted potential research opportunities and gaps based on a review of the literature, which should help steer future research initiatives. [6] In this study, a novel Blockchain-based online social network that considers the user as the central system is proposed. [7] For user autonomy, a decentralized autonomous organization is created, allowing users to democratically self-manage the online social network. [8] Distributed online social networks have the potential to address privacy concerns, but they also introduce inefficiencies in the provision of essential features like data availability and access control. [9] A safe foundation for sharing, retrieving, and accessing data can be achieved with blockchain technology, ensuring privacy and fairness while preventing potential harm to users' interests. [10] Nowadays, where people spend a lot of time exchanging personal information, online social networks are a major means of communication. Regrettably, the largescale use of Internet Social Networks has brought with it considerable privacy concerns. Effective decentralised privacy protection strategies must be implemented in the context of decentralization of social services.

III. GOALS

Provide a safe website where users can keep their digital identities and have their identities confirmed by a verifier. an incentive system to encourage involvement and guarantee the network runs well. Enable trustworthy and safe identity verification for a range of applications, including e-commerce, financial services, and healthcare.

IV. SYSTEM ARCHITECTURE


1. User uploads Identity documents
2. Requesting access to identify documents
3. Notification for allowing access to the vendor
Browser
4. User accepts requests and provide read access
Organization
User
6. If number of documents verified>5 then reward is given
5. Retrieve user data
Blockchain

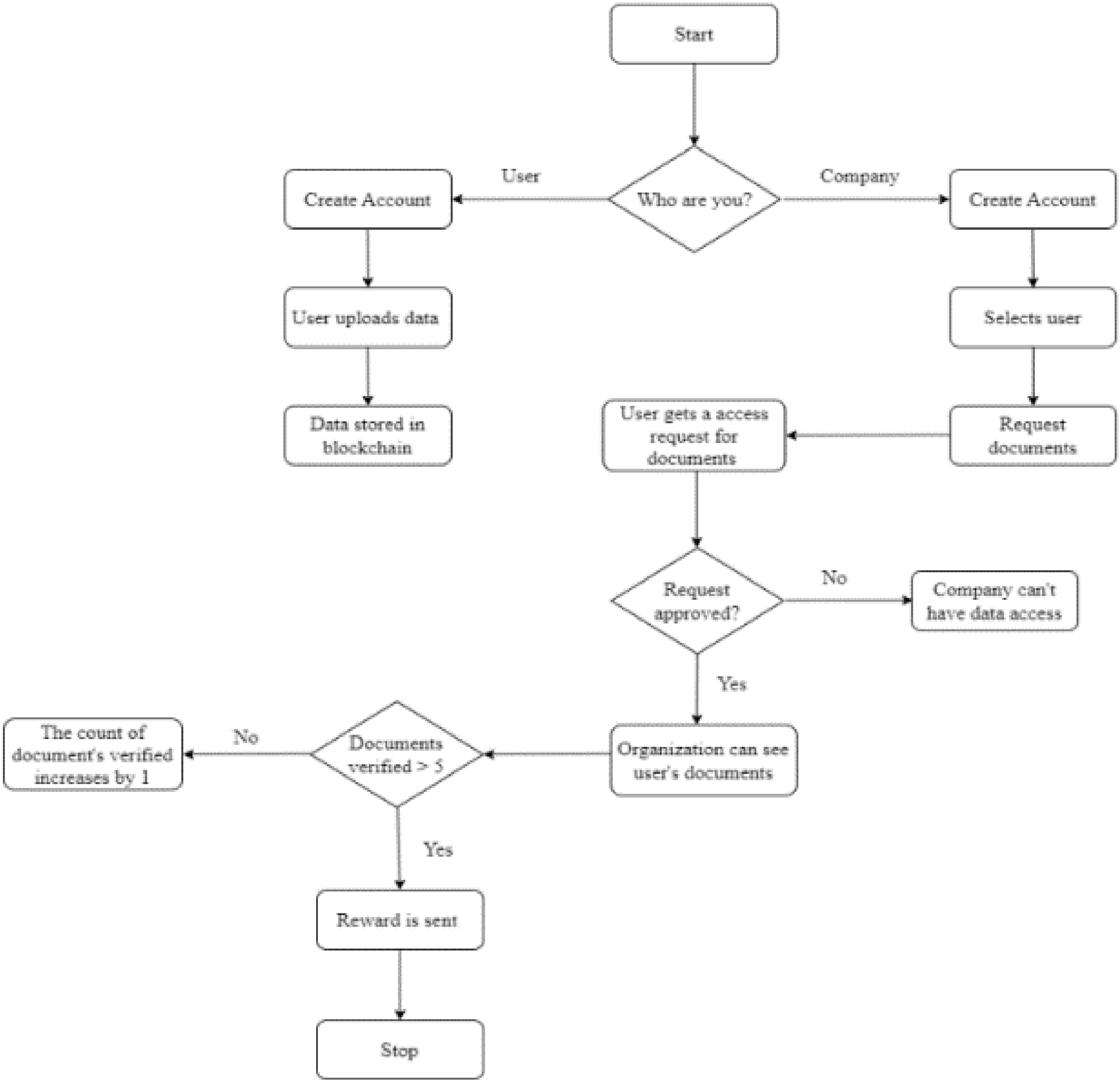
© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IARJSET.2024.11620

The architecture of the system is composed of two sides: users and organisations. Any individual or organization may verify their identity through registration and login. The user will be able to create a profile and upload identification documents, providing an unique key that enables companies to view the individual's documentation. The user must upload their online identities that will be kept in the blockchain after receiving a key.

The data will belong to the user. It assists users in selecting which information to disclose to organizations. Without the user's permission, no data can be shared with any identity seeker. A notification is delivered to the identity owners each time an organization needs access to certain user data for authentication purposes. If the user agrees to have his or her data accessed by companies, third parties may be able to view information about him or her in order to verify identity.

V. FLOW DIAGRAM


Start
Who are you?
User
Company
Create Account
Create Account
User uploads data
Selects user
Data stored in blockchain
User gets a access request for documents
Request documents
Request approved?
No
Company can't have data access
Yes
Organization can see user's documents
Documents verified > 5
No
The count of document's verified increases by 1
Yes
Reward is sent
Stop

Before use our system, users and companies need to register by providing their email address. The blockchain will contain all user and company credentials, to encrypt the password, the hashing function will be used. be used to encrypt the password. Upon approval of the transaction, the hashes will be kept on the blockchain. After creating a hash, we ask which peers' content is at that hash and then we download the data straight from that peer. The business will then ask the person for the necessary paperwork. Once the request has been approved by the individual through an approval email, the company will have access to those papers.

The functional requirements set out what the system or component of software should be capable of doing, as well as specifying its behaviour and capabilities which are necessary. They give users or stakeholders an explanation of the tasks, offerings, or features that the system is meant to fulfil. a straightforward online application that may be easily accessed from any place. Uploading identity documents is easy for users. By sending a request to the user, to access the ID may be requested by the company. If users so want, they can grant access to the company. The identity documents can be verified by the company. Companies who verify a predetermined number of user identity documents are awarded prizes in the form of vouchers, in order to pay the companies that check documents, which may be applied as part of future implementation.

VI. IMPLEMENTATION

Signup/Login for both users and businesses created a login/signup page with JSP that requires users and corporations to provide their email address and password. A MySQL database securely stores the entered data. Using Java code, the implementation validates and processes the data, handles user input through HTML forms, connects to the MySQL database using JDBC, executes SQL queries to insert the data into the relevant table in the database, and with regard to the query execution results, provides user with appropriate feedback. To safeguard user data, security procedures such secure connection protocols and password hashing are used.

Information storage Users may provide their identity details when they are successful in logging on, which are issued by the government. Subsequently, these details are securely stored as blocks within an array on an exclusive blockchain. As part of the custom blockchain implementation, a data structure with the attributes required to represent a block— such as the hash of the previous block, the timestamp, the contents, and a unique identifier—must be generated. Every identity entry adds to the blockchain, forming a chain of blocks linked by cryptographic hashes. This safeguards the immutability and integrity of the recorded user identifying information because any alteration to a block will alter its hash and end the chain. The method uses a customized blockchain to deliver improved data and trust. Blockchain Server: In a blockchain-based system, the security, integrity, and decentralized nature of the identity management process depends on the presence of a blockchain server, which is also referred to as a node. The data relating to the user's identity is encrypted and stored on the blockchain server. Usually, a unique identifier (such a public key) is linked to each user's identification. The identifying information is encrypted on the server. Whenever a user wishes to verify their identification or participate in a transaction, the blockchain server can verify the accuracy of the user's identity by consulting the relevant blockchain records. After creating the user's ID, A user-generated ID is implemented and automatically emailed to the relevant companies to help with the verification of identity document details by companies. The system creates a special key linked to the user's submitted information once they have finished storing their ID. The appropriate companies receive an automated email from the system with the user's ID attached. This email is sent to the company as a notification, giving them the information they need to access and review the user's data. Businesses can quickly consult and obtain the relevant user's data from the system by referencing the key ID in the email. Companies can efficiently verify users' details to this streamlined approach, guaranteeing smooth. Requesting information and granting access to data Companies must obtain the consent of users before accessing their personal information. After the user produces ID information and the firm receives it, the company will contact the user and ask for permission to access his or her information. Usually, a secure communication channel—like email or a specialized portal—is used to send this request. The business describes the aim and extent of About the data access and gives the user explicit advice on how to consent or object. After that, the user can examine the request and decide whether or not to grant access to the data. User privacy is guaranteed by this authorization process, which ensures that businesses can access user data only with the express. Verify the information. Once the organization has the user's key ID, it may enter the ID into the system to obtain the relevant user data. The business can ask the system for the key ID by sending a query over an API or a secure web interface. After that, the system compares the ID with the data that the user has saved and obtains the pertinent details pertaining to that ID. This gives the business access to all of the user's data, including documents, identity data and any additional information that has been provided during the documentation process. This technology enables businesses to meet the requirements and validate user identification by accurately retrieving required details in a timely manner. This process ensures that only approved companies are allowed to operate.

VII. RESULT

In the digital era, blockchain-based social networks for managing user identities have come to light as a ground-breaking solution that improves security, privacy, and effectiveness. In order to provide individuals with more control over their personal information while maintaining its legitimacy and integrity, the decentralised nature of the blockchain technology can be used by identity management systems. Cryptographic protocols and the intrinsic immutability of blockchain technology allows for the creation of digital identities that are impenetrable to fraud, forgery, and unauthorised access.

DOI: 10.17148/IARJSET.2024.11620

Furthermore, users' identities may be validated and verified seamlessly across several platforms and organizations because to the distributed ledger feature of blockchain, which does away with the necessity for recurrent user identity verification procedures. In addition to streamlining the user introduction and authentication procedures, this will reduce costs and improve experience for users. Additionally, user privacy is prioritized by blockchain-based social networks of identity management systems that let people own and control their personal data. Users will be able to control who can access their data and under what conditions, through the disclosure of only parts of their data, while keeping the rest of their data encrypted. With these developments, user identity management on blockchain is set to transform how people communicate and conduct business online by promoting security, autonomy, and trust in the handling of personal identities.

VIII. CONCLUSION AND FUTURE SCOPE

Finally, it is evident that the creation of a Social Network for Users' Identities with Blockchain Technology has tremendous potential to fundamentally change how people manage, verify and protect their identities under modern times. Decentralised, immutable and secured protocols of the blockchain" technology offer a secure and impenetrable platform for private data. By eliminating the need for centralised authority and repetitious identity verification procedures, Blockchain based social network solutions for user identity management provide greater efficiency, lower costs, and better user-experience. Thanks to the emphasis on user privacy and data ownership, individuals are also free to choose what information they make public, maintain their independence and control of personal data. The potential of a social network based on blockchain technology for the management of user identities is bright. Advances like zero-knowledge proofs, decentralized identifiers (DIDs), and self-sovereign identities (SSI) potential to increase privacy, security and interoperability as a result of the next growth. in managing user identification systems as blockchain technology continues to advance. Furthermore, combining blockchain-based social network of users' identity management solutions with other cutting-edge technologies like artificial intelligence (AI), biometrics, and Internet of Things (IoT) new opportunities for secure and seamless digital interactions can be created. But there are still issues to be resolved, including as scalability, legal frameworks, and closing the digital gap. To get beyond these challenges, industry leaders, legislators, and technological innovators should work together to guarantee that blockchain-based social networks for user's identity management systems, they are widely used and standardised. User's identity management using the blockchain is going to transform the digital world. In the digital real, it will give people power, build confidence and allow safer interaction.

REFERENCES

[1]. Title of the work: Digital Identity Management System Using Blockchain Citation: Devi, Sulochana and Kotian, Shrineeth and Kumavat, Manish and Patel, Dixit, Digital Identity Management System Using Blockchain (April 3, 2022).

[2]. Title of the work: Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use- Cases, and Comparative Study.

[3]. Title of the work: Identity Management Systems: A Comparative Analysis. Citation: JOUR, Kumar Vikas, Bhardwaj & Aashish. Published Year(2018/1/1).SP – 63 EP- 78.JO-International Journal of Strategic Decision Sciences.T1- Identity Management Systems: A Comparative Analysis.

[4]. Title of the work: A survey on blockchain-based identity management and decentralized privacy for personal data Citation : Komal Gilani, Emmanuel Bertin, Julien Hatin, Noel Crespi. A survey on blockchain- based identity management and decentralized privacy for personal data. BRAIN 2020: 2nd conference on Blockchain Research & Applications for Innovative Networks and Services, Sep 2020, Paris, France.

[5]. Identity management system - Privacy and Security Aspects Citation : Andreea-Elena PANAIT, Ruxandra F. OLIMID, Alin STEFANESC.

[6]. Barbara Guidi "When Blockchain Meets Online Social Network" Pervasive and Mobile Computing Volume 62, February 2020.

[7]. Ningyuan Chen, David Siu-Yeung Cho "A Blockchain Based Autonomous Decentralized Online Social Network" paper published in 2021.

[8]. IEEE Transaction on Computational Social Systems "A Blockchain-Based Decentralized Online Social Network" IEEE Transaction on Computational Social Systems (Volume: 6, Issue: 6, December 2019).

[9]. Shiwen Zhang, Tingting Yao, Vaundi Koe Arthur Sandor "A novel blockchain-based privacy-preserving framework for online social networks" Revived on 21st July 2020, accepted on 8th Nov 2020, Published online on 7th January 2020.

[10]. Mohsin Ur Rahaman, Barbara Guidi, Fabrizio Baiardi "Blockchain-based access control management for Decentralized Online Social Networks" Received 14 October 2019, Revised 15 April 2020, Accepted 21 May 2020, Available online 4 June 2020, Version of Record 9 June 2020.