www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 1174-1178

e-ISSN : 2583-1062
Impact Factor : 7.001

A SURVEY PAPER ON DIGITAL IDENTITY VERIFICATION – A BLOCKCHAIN-BASED SYSTEM FOR VERIFYING AND MANAGING DIGITAL IDENTITIES

Diksha Sanjay Gurav[1], Shreya Ramkrishna Gurav[2], Anushka Sanjay Mate[3], Mayuri Mahendra Kumbhar[4], Prof. Vijay B. Mohite[5]

[1,2,3,4,5]Zeal Polytechnic, Pune, India.

ABSTRACT

Today, the world increasingly relies on digital means for identification, verifying identities has become more complex and critical due to the increasing cases of identity theft, breaches and fraud. Normal methods for identification verification are often centralized in a server, therefore posing significant dangers and threats for the users. In this regard, we discuss the introduction of the digital identity management and verification system based on blockchain technology as an efficient way to mitigate the above-mentioned issues utilizing decentralization, immutability and encryption capabilities of the blockchain technology. Basing on the literature, we map relevant and critical gaps- regulatory and legal barriers, the need to connect with legacy systems, and the need to attract users- and offer a valuable mix of decentralized identity, smart contracts and credentials that are backed up by the merits of verifiable technologies. We conclude that specific approaches of the new technologies of identity exchange based on Blockchain not only guarantee the protection of data and privacy goals, but tend to streamline the verification process itself making it mobile and user friendly. The significance of this research is great bearing in mind the sensitive nature of the knowledge in sectors like finance, health and government services amongst others where identification of a person is important. This research continues the investigations of how digital identity can be managed, its opportunities based on the blockchain technology while calling to address the difficulties and opportunities of the domain.

1. INTRODUCTION

Today's world is more interconnected than ever, and as a result of this, digital identity has become integral to most online communications, interactions and transactions, be it through social networking, finances and even healthcare. Existing conventional identity verification systems are heavily dependent on centralized identity systems and databases operated by corporation and governments, which creates an avenue for users' identity to be compromised, resulting in rascality such as identity theft and leaks of confidential data. Most of these have enforced a policy where the end users are required to provide these details which are on the Event Timeline, which has the risk of data abuse or leaking, in this case, explaining the need for newer and safer networks. Is there anything new in this? In as much as users deposit their identity details and pay their taxes electronically which is an NGO e-citizen approach, there is a distinct patience and expectation for thinking of a way out of the boxed solutions every time. Unlike the conventional identity verification systems, blockchain technology brings good returns. Such development ensures that there are no single points of failure in any system, hence rationalizing data redundancy further strengthening data security. Each user of the system can have digital ownership of their identity based on the decentralized identity model, where proof of identity can be provided by an individual but their particulars remain private. Moreover, with the availability of smart contracts and verifiable credentials, the process of competing verification can also be done automatically, hence minimizing the chances of human error and speeding the transactions. In essence, this paper intends to go into the details of those innovations of the digital identity management comparing the organic way in which changes can be brought on board that enhance the issues with traditional systems embracing security and trust in online relations and interactions. The value of this research is not limited to innovation; it is of utmost importance to several industries such as finance, healthcare, and government that call for heavy identity purposes. With organizations working towards increasing the trust of users and meeting the ever increa0sing mandates on data protection, a transition to blockchain-based identity solutions could become inevitable. In this paper, the literature on today's identity verification will be reviewed, essential problems will be identified, and a detailed incorporation of a blockchain system will be recommended which will contribute in one way or the other e to the developing debate on the digital identity and its likely impact on enhancing online safety.

2. LITERATURE SURVEY

The understanding and handling of the content concerning how the identity verification online has advanced over the years providing different means to properly meet the concerns related to security, privacy and usability of these approaches. The conventional means of establishing identity have relied on the use of personal information stored in set up databases. Though effective, these systems have attracted a lot of negative remarks due to their drawbacks.

Smith (2020) points out that all centralized databases are prone to a defense in depth failure which is the reason why hackers love them so much. It is not uncommon to hear of data leaks such as them where the private details of millions of users are placed out on the web leading to the need to shift the focus on how people are identified in the cyberspace. Thus, the question is what happens with such an assessment in case blockchain technologies are applied. No longer is the issue of identity data held by one entity who then bears all risks accompanying such storage, because the system is distributed. It is cryptocurrency that has used the first concept of blockchain laid out by Nakamoto (2008) in the bitcoin. Blockchain is also relevant to understanding the infrastructure of cryptocurrencies sip (Tapscott and Tapscott 2016). Their research offers interesting insights into how this traceability and permanence can increase the trust of users because any modification of the identity information stored in the blockchain is available to every single user on the network such as in a traditional system where there is 'no' such audibility, as it is requested all the time, it is impermanent.

Recent developments have made it possible to focus attention and effort on decentralized identity (DID) frameworks that give full control of identity management to the end- user. W3C (2020) conceptualizes DIDs as convenient orientations that prohibit mistreatment of individuals and their claimed digital identities. The trend of providing such features to the users is also pointed out by Allen (2016), who stresses the need for self-sovereign identity models that allow users to control the amount of information to be disclosed while owning that information. There are also regulations that support such models like GDPR, which makes sure that user's privacy and their consent to data usage is prioritized.

Verifiable credentials have emerged as a serious aspect of identity systems within blockchain environments. Mastorocostas et al. (2021) explain how these credentials, stored electronically on blockchain and signed, allow for proof of identity in ways that do not require people to disclose sensitive information. This feature resolves an annoying problem in valuable systems where an individual is required to provide a lot of information about themselves in order to verify their identity. Employing the techniques of digital guardians who preserve users' trustworthy anonymity, verifiable credentials assist user claims pertaining to certain attributes being age or citizenship, instead of user full identity being presented forging diversity supervision.

At last, the theoretical models for identity management systems based on blockchain technology began to be implemented in practice. Kumar et al. (2022) examine a number of specific instances where this technology has been harnessed in different industries such as finance, health services and the public sector in order to improve the efficiency of identity verification processes. Such implementations not only demonstrate what can be done with such technology, but also shows what more needs to be done, including compliance to regulations, and understanding by the users. With more organizations appreciating the need for digital identity management, the application of blockchain within the self-sovereign identity paradigm may be a game-changer in safeguarding personal information and building trust within virtual environments.

Problem Statement:

In the increasingly interconnected digital world, traditional methods of identity verification, which rely on centralized systems and databases, are vulnerable to various threats such as identity theft, data breaches, and privacy violations. These methods often fail to provide adequate security and trust, as they place the responsibility for managing sensitive user information on a single entity, increasing the risk of data compromise. With rising concerns around personal data protection and regulatory requirements like GDPR, there is a growing need for a more secure, decentralized, and user-controlled system for managing digital identities.

This survey paper seeks to explore how blockchain technology, with its decentralization, immutability, and cryptographic capabilities, can revolutionize digital identity management. By analyzing existing literature, this paper will map out the critical gaps in current identity verification systems, such as regulatory and legal barriers, integration with legacy systems, and user adoption challenges. The paper will also highlight how blockchain-based identity solutions, including self-sovereign identity models, smart contracts, and verifiable credentials, offer a more secure, privacy-preserving, and efficient method for identity verification.

Through this research, we aim to provide a comprehensive overview of the advancements in blockchain-driven digital identity systems and identify key areas that require further development to ensure their practical implementation across sectors like finance, healthcare, and government services, where secure identity verification is paramount.

Proposed Solutions:

To address the vulnerabilities and limitations of traditional, centralized identity verification systems, a blockchain-based decentralized digital identity management solution is proposed. This solution harnesses the key characteristics of blockchain technology—such as decentralization, immutability, cryptographic security, and transparency—to create

a secure and privacy-preserving framework for identity verification. In this system, users gain full control over their digital identities through a self-sovereign identity (SSI) model, which allows them to own and manage their personal data without depending on a central authority.

A major aspect of the proposed solution is decentralized identity management. By utilizing decentralized identity (DID) frameworks, individuals can store their identity data on the blockchain, eliminating the need for a single entity to control or hold sensitive information. This approach reduces the risk of centralized data breaches and empowers users to retain control over their personal data. Additionally, the system employs verifiable credentials, which are cryptographically signed proofs that allow individuals to verify specific aspects of their identity—such as age, citizenship, or qualifications—without disclosing their full identity. These credentials can be securely and easily verified by third parties, ensuring both privacy and security.

The use of smart contracts further enhances the system by automating the identity verification process. When a user's identity needs to be verified, smart contracts can automatically validate the necessary credentials without human intervention, thereby improving the speed and accuracy of the verification process. Furthermore, blockchain's immutability and encryption mechanisms ensure that identity data is securely stored and accessible only to authorized parties. The system also complies with data protection regulations such as GDPR, giving users control over how and when their information is shared, thereby safeguarding their privacy.

Algorithm for Implementing a Blockchain-based Decentralized Identity System:

1. **Develop Decentralized Identity Framework:**
- Set up a blockchain network supporting DID standards (e.g., W3C DID).
- Create a system where users generate and own their DIDs with minimal intermediaries.
- Build a user-friendly app for managing DIDs, enabling users to control and update their identity data.

2. **Design Verifiable Credentials Infrastructure:**
- Implement a mechanism for trusted authorities to issue cryptographically secure credentials (e.g., licenses, certificates).
- Build a validation process allowing third parties to verify credentials without accessing full identities, using cryptographic techniques.

3. **Integrate Smart Contracts:**
- Develop and deploy smart contracts to automate identity verification based on pre-set conditions (e.g., age, nationality).
- Automate credential validation and manage exceptions (e.g., expired credentials).

4. **Enhance Privacy and Compliance:**
- Implement Zero-Knowledge Proofs (ZKPs) to verify attributes without revealing personal data.
- Ensure GDPR compliance by giving users control over their identity data, with options for revocation and consent-based sharing.

5. **Integrate with Regulations and Legacy Systems:**
- Collaborate with regulators to meet legal requirements and overcome barriers.
- Develop APIs or middleware to integrate the blockchain system with legacy systems (e.g., banking, healthcare).

6. **Pilot and Testing:**
- Pilot the system in sectors with high identity verification needs (e.g., finance, healthcare).
- Test system reliability across various devices and environments, addressing any vulnerabilities.

7. **User Education and Adoption:**
- Create intuitive user interfaces for managing DIDs and credentials.
- Educate users on secure digital identity management through campaigns and resources.

3. PROPOSED SYSTEM ARCHITECTURE

Components:

1. User Registration
2. Issuance of Verifiable Credentials (VCs)
3. Data Storage (Distributed Ledger)
4. Verification Request (API)

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 10, October 2024, pp : 1174-1178
e-ISSN : 2583-1062
Impact Factor : 7.001

5. Privacy-Preserving Verification (Zero-Knowledge Proofs, ZKPs)
6. Verification Outcome

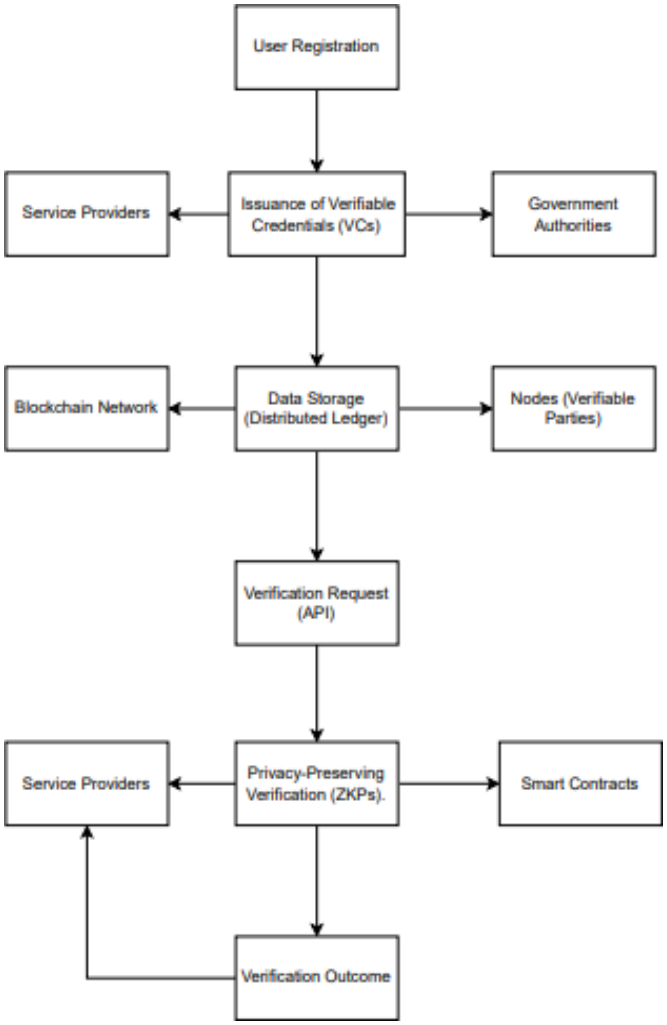

Fig:1 System Architecture

Project and Scope:

This project undertakes the task of creating a digital identity verification system that is based on blockchain technology to improve the security and efficiency of identification as well as increase the control of users over their identity. The system will make use of decentralized identity (DID) so that the users can create, own and manage their identities without the need for centralized databases. There will also be the employment of smart contracts to self' verify process and verifiable credentials to ease identity verification. This project will also address the issue of users' usability by creating an appealing interface that will allow individual users or organizations to interact with the system and ease the registration process.

Scope

The scope of this project entails a number of different threads of work. First of all, it will include thorough qualitative and quantitative analytics of various identity verification methodologies and also of the blockchain technologies in order to foresee the benefits and challenges. Second, the project will also involve building up of the developed system pistachio and cypher with basic and advanced functionalities which include among others decentralized identification, smart contracts, and verifiable credits. Also, the scope will include evaluating the deployed systems in terms of performance, usability and security nurse on test beds.

Critical Evaluation:

The blockchain-based system of digital identity verification proposed in the paper outlines several strengths and potential challenges worthy of critical consideration. On the bright side, the decentralized architecture increases the security of the system because single points of failure have been eliminated, hence lowering the chances of data breaches and identities being stolen. With control over personal information improved, users can manage and selectively disclose their identities using DIDs and verifiable credentials. Nevertheless, regulatory compliance and

interoperability with systems currently in place continue to be issues. The plethora of differing laws regarding data protection across jurisdictions adds complexity and gives a view that an easily implemented universally acceptable solution will be difficult, and integration with more traditional modes of identity verification is likely to require considerable co- operation and standardization measures. User adoption will be a threat; the benefits which blockchain technology has to offer may not cut across easily due to misunderstanding and lack of trust in the potential users.

In general, although the project promises digital transformation, it will need to strategically approach some of these challenges to ensure successful implementation and user acceptance.

4. SIGNIFICANCE

Blockchain-based identity management offers several advantages over traditional centralized systems. First, better security is achieved through decentralization, which eliminates the risk of data theft and identity crimes by removing central points of vulnerability. Empowerment of users is another key benefit, as decentralized identities (DIDs) allow individuals to take control of their personal information, deciding how much to share and with whom, without relying on intermediaries. Additionally, privacy preservation is maintained through the use of verifiable credentials and advanced cryptographic techniques. This enables users to prove attributes like age or citizenship without revealing sensitive information, ensuring that their privacy is protected.

Moreover, the implementation of smart contracts simplifies identity verification processes, automating tasks and reducing human error, while increasing efficiency in sectors such as finance and healthcare. The system can also be built to ensure compliance with global data protection regulations, such as GDPR, reinforcing trust in digital transactions by safeguarding users' rights. With cross-sector applications, this solution can address identity verification needs across industries like finance, healthcare, and government, offering broad utility.

The decentralized approach also helps in reducing identity fraud, providing a secure and reliable method of identity verification for both users and organizations. Finally, cost efficiency is another important benefit, as the technology reduces operational costs associated with managing and verifying identities, leading to significant savings for organizations.

5. CONCLUSION

This initiative presents a realistic modern way to address the risks of identity management systems, by offering a more secure and efficient… system. Implementing key aspects of blockchain like immutability and smart contracts enhances security of the identity management system and ensures provision of civilized' treatment to users. This enhances the security of data as a self- sovereign identity is offered, increases the level of consumer confidence by offering verifiable credentials, and brings in augmentability and interoperability with other technologies. There are still issues of acceptance of the system, adherence to the laws, the dimensionality of the system and other gaps… given the system however, represents a new concept, and a bright prospect for the effective verification of digital identity in the near future applicable across several industries.

6. REFERENCES

[1] Zhiming Song, Guiwen Wang, Yimin Yu, and Taowei Chen (2022). "Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior".

[2] B. Angel Rubavathy, Rebecca Jeyavadhanam Balasundaram, S. Albert Antony Raj. Blockchain Based Secure Digital Identity Verification System for Robust Documents.

[3] Feng Wang, Yongjie Gai, Haitao Zhang. Blockchain user digital identity big data and information security process protection based on network trust.