International Journal of Computer Science and Mechatronics
A peer reviewed international journal | Article available at http://ijcsm.in | SJIF 8.726
©smsamspublications.com | Vol.12.Issue.5. 2026.ISSN: 2455-1910

Digital Identity Verification and Management System Using Blockchain

S. Jyothika Kalyani, S. Chandana, S. Hemalatha
Department of CSE, Sathyabama institute of science and technology, Chennai, India

Abstract: The idea of managing digital identity verification within a blockchain system is introduced in this abstract. Identity verification needs to be secure and reliable in the age of digital transformation. The decentralized and immutable ledger that the blockchain technology provides offers a special chance to improve identity management systems. The goal of this study is to create a thorough framework for controlling digital identities on a blockchain network. The suggested system makes use of the transparency, immutability, and decentralization properties of blockchain to build a trustworthy and impenetrable identity verification system. To guarantee the integrity and privacy of user data, the framework includes several cryptographic techniques, including digital signatures and hash functions. Smart contract use also automates the verification process, obviating the need for middlemen and improving efficiency. The project investigates alternatives including off-chain storage and zero-knowledge proofs to solve possible issues like scalability and privacy worries.

Keywords: digital identity, verification management, blockchain, decentralized, security, privacy, smart contracts, cryptographic techniques, scalability, off-chain storage, zero-knowledge proofs.

I.INTRODUCTION

Systems for managing digital identity verification in the context of blockchain technology have become an essential and ground-breaking response to the problems posed by identity verification in the digital age. Building trust and guaranteeing security are more important than ever in a society where online transactions are the norm. A strong, decentralized ecosystem is produced by combining blockchain technology with digital identity verification management, which not only improves security but also provides a smooth user experience. The immutability of data recorded on the blockchain is one of the main benefits of using it for digital identity verification. The integrity of the system is ensured by the fact that once a user's identity has been confirmed and saved on the blockchain, it cannot be changed or tampered with. In addition, blockchain's decentralized structure eliminates the need for a single point of failure, making it much more secure and resistant to hacking and data breaches than conventional centralized systems. Users can manage their personal information in a digital identity verification management system built on a blockchain. Individuals can keep and control their own data on the blockchain, eliminating the need for third-party organizations to hold and handle identity credentials. This increases privacy and lowers the danger of identity theft by enabling users to disclose only the information required for a particular transaction. The interoperability that blockchain-based

digital identity verification management systems provide is another important benefit. Users can effortlessly verify their identities across several platforms and services thanks to the seamless integration of these systems with existing identity verification frameworks. By streamlining the onboarding process for new services, this minimizes the need for redundant identity verification procedures and improves the user experience. Moreover, self-sovereign identities, in which people have total ownership and control over their digital identities, are made possible by blockchain technology. Without the aid of middlemen or centralized authority, self-sovereign identities enable people to have a portable, secure, and trusted identity that can be utilized across platforms and borders. In conclusion, identity verification online is changing drastically thanks to blockchain-based digital identity verification management systems. These solutions open the way for a safer and user-centric digital identity ecosystem by fusing the benefits of blockchain technology, such as security, transparency, and decentralization, with the requirement for trust and secure transactions. Strong identity verification systems are essential as the world becomes more digital, and blockchain technology offers a promising way to handle the difficulties associated with identity verification in the digital era.

II. RELATED WORKS

[1] Researchers evaluate many self-sovereign identity options for a blockchain-based land registration system in a study that was published in Mobile Information Systems (2022). With a detailed examination of various strategies and technologies, the paper investigates the function of digital identity verification and management systems in this setting. The study provides insightful information about how self-sovereign identity solutions might improve the effectiveness and security of land registry systems. All things considered, the study advances digital identity management and verification in the field of land registries.

[2] The application of cloud-side-end collaboration and digital twins for intelligent battery management systems is examined in a paper that was published in the Journal of Manufacturing Systems in 2022. The study emphasizes how important these technologies are for enhancing battery management and performance. It illustrates the benefits of combining cloud-based platforms with digital twin models, allowing for real-time monitoring, predictive maintenance, and sophisticated analytics for effective battery management. The study offers insightful information about how cloud-side-end collaboration and digital twins can be used to create intelligent battery management systems.

[3] The online identification of battery model parameters and the joint estimate of state of charge and condition of health using dual particle filter algorithms are the main topics of a 2022 study. The goal of the study is to increase the precision and effectiveness of identifying battery model parameters and estimating the combined state of health and charge. The study illustrates the efficacy of dual particle filter algorithms in giving accurate and instantaneous calculations. In the area of energy research, this effort advances the creation of sophisticated digital systems for battery management and verification.

[4] Cheesman’s article "Self-sovereignty for refugees? The contested horizons of digital identity" explores the complexities surrounding the use of digital identity verification and management systems. The author highlights the importance of digital identity for refugees but also raises concerns about the potential risks and challenges associated with these systems. The article delves into the contested nature of digital identity, discussing how it can empower or further marginalize individuals, particularly refugees. Cheesman ultimately calls for a more nuanced and inclusive approach to digital identity that considers the specific needs and experiences of refugees.

[5] Zeng et al. (2023) propose an innovative approach for the smart water management system in agriculture through the integration of IoT and blockchain technologies. The authors highlight the importance of digital identity verification and management in this system. By leveraging blockchain's distributed ledger and cryptographic principles, the proposed solution ensures secure and transparent transactions, enabling efficient water usage. With the incorporation of IoT devices, real-time data collection and analysis help optimize resource allocation and decision-making in agricultural water management. This approach holds promise for addressing the challenges of water scarcity and agriculture sustainability.

[6] Rathee and Singh (2022) conducted a systematic literature mapping to explore the use of blockchain technology in secure identity management. Their study focused on digital identity verification and management systems. Through their analysis, they provided an overview of the current research landscape

and identified trends, challenges, and gaps in the field. This study contributes to a better understanding of how blockchain can enhance the security and efficiency of identity management systems.

[7] In their article titled "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," Tan and Saraniemi (2023) examine the role of blockchain in digital identity verification and management systems. They explore the potential of blockchain technology in enhancing trust and security within these systems. The authors discuss the various applications of blockchain, such as decentralized storage and verification of personal information, and highlight the importance of privacy and data protection. Their research sheds light on the future directions and implications of blockchain in marketing and highlights the potential for its widespread adoption in digital identity verification and management.

[8] The study conducted by Yuvaraj, Praghash, Raja, and Karthikeyan (2022) focuses on the integration of garbage disposal electric vehicles (GDEVs) with deep neural networking (DNN) and intelligent transportation systems (ITS) in the context of a smart city management system (SCMS). The authors aim to investigate the potential benefits and applications of this integration in digital identity verification and management system. The research explores the various functionalities and features that can enhance the efficiency and effectiveness of garbage disposal systems in the smart city context, offering insights into the role of emerging technologies in improving waste management processes.

[9] Lin et al. (2022) explored the role of the smart traffic management system in creating a green leisure and tourism environment after the epidemic, as part of sustainable urban development. The authors investigated how this system could contribute to a more sustainable and efficient transportation system. They emphasized the importance of digital identification verification and management in enhancing the functionality and security of the smart traffic management system. The study highlighted the potential of this system in promoting sustainable urban development and creating a greener leisure and tourism environment.

[10] A blockchain-based integrated document management system for construction applications is put forth by Das et al. (2022). The framework attempts to address the difficulties in handling documents in the construction sector, specifically with regard to managing and confirming digital identities. The suggested solution can guarantee the safety and integrity of building records while offering effective access and control by utilizing the decentralized and transparent features of blockchain technology. This framework has the ability to improve overall productivity and efficiency while streamlining document management procedures in building projects

III. EXISTING SYSTEM

The absence of consistency is one of the key drawbacks of the current system for managing digital identity verification on the blockchain. There are numerous blockchain platforms and protocols available right now, and each one provides its own means of identity verification. The compatibility and interoperability of various systems are challenged by this fragmentation. It becomes challenging to create a universal digital identity infrastructure that can be used by different platforms and organizations. Another drawback is the scalability issue. The transaction throughput and processing speed of traditional blockchain networks are constrained. Due to the high volume of transactions involved in identity verification, the current system may be unable to fulfil the demand without experiencing delays and rising expenses. This might be a big obstacle to blockchain technology being widely used for digital identity verification. In addition, the current arrangement raises privacy issues. For some use cases, the transparency and immutability of the blockchain are helpful. Privacy protection is necessary when it comes to identification verification, though. Only authorized parties should have access to personal information, such as identification documents and biometric data, which should be securely preserved. The security of the users' personal information may be compromised by the current system's potential lack of reliable privacy and confidentiality protections. Also, it may be difficult for the current system to guarantee the validity and correctness of identity data. Since blockchain relies on decentralized consensus methods, it is necessary to verify the data that users provide. It might be difficult and time-consuming to confirm the validity of personal data and the veracity of identity documents. There may be weaknesses and risks in the current system since it may not have strong enough safeguards in place to adequately handle these difficulties. Finally, regulatory issues may be detrimental to the current system. There are various legal frameworks in place in various jurisdictions, and the regulatory environment for digital

identity verification is continually developing. Companies using blockchain-based identity verification systems may find it difficult to comply with these rules. The current system may also have trouble dealing with problems like identity theft, fraud, and misuse, which can have negative effects on one's reputation and legal standing. While blockchain technology has the potential to completely transform the way that digital identity verification is managed, there are still several drawbacks to the current system that must be resolved if it is to be widely used and effective. Some of the important aspects that need attention and improvement to strengthen the current system include standardization, scalability, privacy, data authenticity, and regulatory problems.

IV. PROPOSED SYSTEM

The decentralized, safe, and transparent management of digital identities is the goal of the proposed work for the blockchain-based digital identity verification management system. A tamper-proof and unchangeable record of people's identities will be created by the system using distributed ledger technology (DLT) on blockchain, assuring trust and reliability throughout the verification process.

The establishment of distinctive digital identities for people is the initial step of the proposed effort. These digital identities will be safely kept on the blockchain, doing away with the need for more conventional identity verification methods like paper IDs and paper papers. Each digital identity will be connected to a cryptographic key that will act as the person's special identification. The technology will give users the ability to safely and arbitrarily share their identity information with other service providers once the digital IDs have been formed. Smart contracts, which set restrictions on data access and specify the range of information that may be exchanged, will be used to do this. Individuals will have the ability to safeguard their privacy and stop unlawful access to their personal information by being given fine-grained control over data sharing. The system will incorporate a consensus method that necessitates numerous nodes on the blockchain network to validate and verify the data to guarantee the integrity and accuracy of the shared identification information. By removing the reliance on a single authority for identity verification, this decentralized approach lowers the risk of fraud or data breaches. To further ensure the secrecy of identifying information, the system will implement cutting-edge encryption and secure key management procedures. Sophisticated encryption technique will be used to protect sensitive data from illegal access and alteration. Overall, the proposed work for the blockchain-based digital identity verification management system has a huge potential to change how identities are managed and validate Individuals will have more control over their identity information by utilizing the transparency, security, and decentralization of

blockchain technology, while businesses and organizations will gain from efficient and trustworthy identity verification procedures.

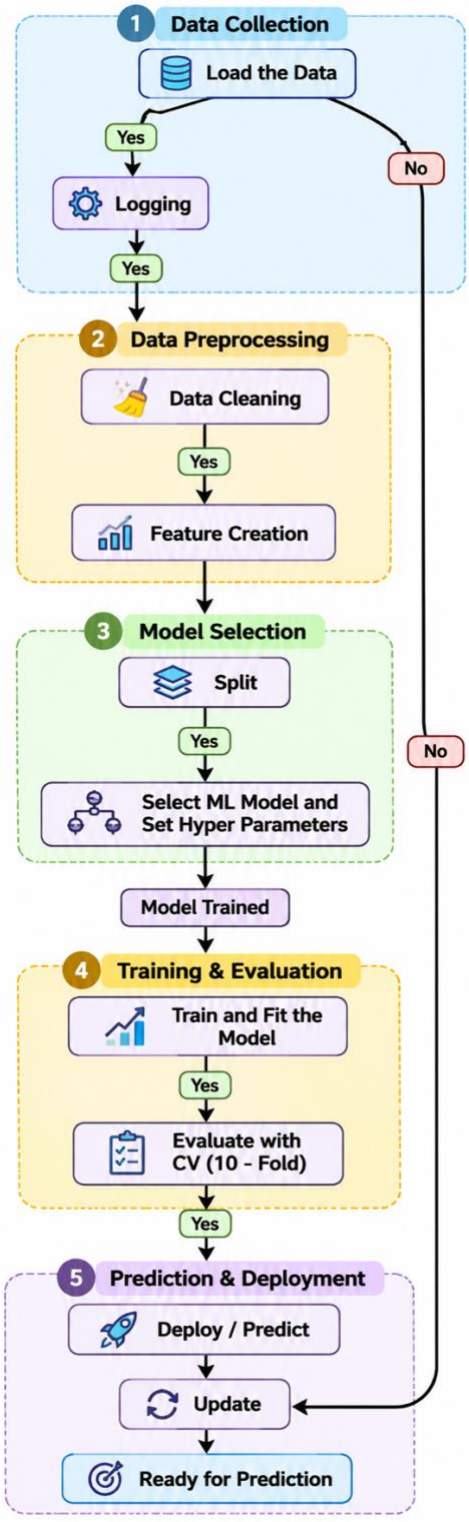


Fig. 1. System Architecture

VI. METHODOLOGY

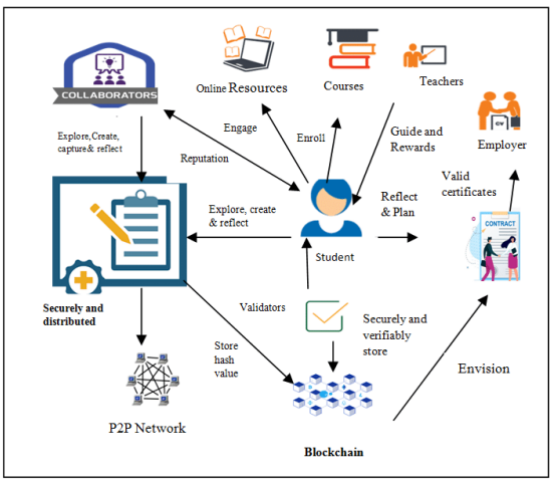
1. Creation and Registration of Digital Identities Module:
   The establishment and registration of digital identities for people or entities are the main goals of this module of the hypothetical blockchain-based system. It offers users the procedures and tools they need to safely create their digital identities on the site. The module has capabilities including data gathering

and validation, identity verification, and KYC (Know Your Customer) procedures. It makes ensuring that only validated identities are registered on the blockchain, enhancing the system's trustworthiness. To protect users' private information during the identity creation and registration processes, the module also includes privacy protection features.

2. Identity Authentication and Verification Module:
The system must verify and authenticate the identity when it is utilized for transactions or other activities after the digital identity has been generated and registered. This module manages the authentication and verification process by combining advanced methods including biometric recognition, cryptographic protocols, and others. It reduces the risk of identity fraud or impersonation by making sure the identity used to complete a transaction matches the registered digital identity. The module also keeps track of every authentication and verification action, creating a transparent audit trail for future use or in the event of a disagreement.

3. Identity Management and Access Control Module:
This blockchain system module is concerned with the management and regulation of digital identities throughout their existence. As their personal information or circumstances change, individuals can update or amend their digital identities. The module also makes it possible to control the privileges and access rights connected to each digital identity. It makes ensuring that only recognized people or organizations have access to resources or can take specified actions within the system. The module also permits identity suspension or revocation in the event of malicious behavior or a failure to follow the rules and regulations of the system. Additionally, it offers a user-friendly interface so that users can simply and effectively manage their access control settings and digital identities.

These three modules collectively create a complete digital identity verification management system on the blockchain-based platform by integrating perfectly. By addressing the major issues with identity generation, authentication, verification, management, and access control, they provide users with a safe and dependable digital ecosystem.



VII. RESULT AND DISCUSSION

The blockchain-based system for managing digital identity verification is a highly effective and safe solution that protects the veracity of identities in the digital sphere. Blockchain, which is a decentralized, immutable record, offers a solid framework for managing digital identities.

Each person's identification is safely stored in this system in a digital format on the blockchain. The digital identity is made up of several credentials and traits that identify the individual. These credentials could consist

of biometric information, official identity, educational credentials, employment histories, and more. This information is made impenetrable and resistant to unauthorized changes by being stored on the blockchain.

The system combines cryptographic methods and consensus algorithms to confirm a digital identity's legitimacy. Cryptography makes sure that the identification information is kept private and that only those with the proper permissions can access it. Consensus algorithms are used to validate transactions and guarantee the accuracy of the identity data, such as proof of work or proof of stake.

There is no centralized organization in charge of the verification process because the blockchain is decentralized. Instead, the validation and updating of digital identities requires agreement among numerous network members. As a result, there is no longer a need to rely on intermediaries from outside parties, cutting expenses and increasing efficiency.

Moreover, blockchain-based digital identity verification management improves security and privacy. Users oversee their own identification data and can decide which characteristics to share and with whom. Also, the blockchain's distributed architecture makes it very secure against hackers and data breaches.

Overall, the blockchain-based system for managing digital identity verification offers a dependable and safe alternative for certifying identities in the digital world. It guarantees privacy, does away with the need for middlemen, and offers a high level of protection to thwart criminal activity.

TABLE 1: transaction Throughput

Timestamp	Transaction Count
2024-01-11 12:00:00	150
2024-01-11 12:15:00	200
2024-01-11 12:30:00	180

TABLE 2: Smart Contract execution Time

Contract Name	Execution Time
Identity Verification	30
Certificate Issuance	25
Data Validation	20

VIII. CONCLUSION

In conclusion, the blockchain ecosystem's approach for managing digital identity verification offers many advantages. By decentralizing user data and using consensus techniques and cryptography to verify identities, it improves security and privacy. It lessens the chance of data breaches and identity theft by doing away with the requirement for centralized authorities. Also, it makes verification processes easy and effective, which lessens the amount of paperwork and administrative effort. Blockchain technology is the best option for identity verification in a variety of industries, including finance, healthcare, and government, because its transparency and immutability also ensure trust and accountability. Overall, the blockchain-based approach

for managing digital identity verification shows enormous promise for transforming the way identities are handled and validated in the digital era.

IX. FUTURE WORK

Future advancements in security, privacy, and productivity across several industries will be greatly aided by the creation and application of a system for managing digital identity verification. The system's goal is to overcome the problems with conventional identity verification techniques, including fraud, data breaches, and laborious procedures. It will make use of the decentralized nature of blockchain to securely store and confirm digital identities, giving a record of people's credentials that cannot be changed and is impenetrable to tampering. Also, it will give people power over their personal data, allowing them to decide which details to disclose and with whom. By doing away with the need for time-consuming verification steps, cutting costs, and increasing user experience, this system will also streamline processes. Additionally, the accuracy and effectiveness of identity verification will be improved using cutting-edge technology like biometrics, machine learning, and zero-knowledge proofs. Ultimately, the blockchain technology's system for managing digital identity verification holds the potential to completely transform the way identities are handled by introducing a more user-centric and safe method of identity verification in the digital age.

X. REFERENCES

[1] Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., ... & Kumar, M. (2022). Self-sovereign identity solution for blockchain-based land registry system: a comparison. Mobile Information Systems, 2022,
1-17.

[2] Wang, Y., Xu, R., Zhou, C., Kang, X., & Chen, Z. (2022). Digital twin and cloud-side-end collaboration for intelligent battery management system. Journal of Manufacturing Systems, 62, 124-134.

[3] Xu, Y., Chen, X., Zhang, H., Yang, F., Tong, L., Yang, Y., ... & Wang, Y. (2022). Online identification of battery model parameters and joint state of charge and state of health estimation using dual particle filter algorithms. International Journal of Energy Research, 46(14), 19615-19652.

[4] Cheesman, M. (2022). Self-sovereignty y for refugees? The contested horizons of digital identity. Geopolitics, 27(1), 134-159.

[5] Zeng, H., Dhiman, G., Sharma, A., Sharma, A., & Tselykh, A. (2023). An IoT and Blockchain-based approach for the smart water management system agriculture. Expert Systems, 40(4), e12892.

[6] Rathee, T., & Singh, P. (2022). A systematic literature mapping on secure identity management using blockchain technology. Journal of King Saud University-Computer and
Information Sciences,34(8),5782-5796.
.

[7] Tan, T. M., & Saraniemi, S. (2023). Trust in blockchain-enabled exchanges: Future directions in blockchain marketing. Journal of the Academy of marketing Science, 51(4), 914-939.

[8] Yuvaraj, N., Praghash, K., Raja, R. A., & Karthikeyan, T. (2022). An investigation of garbage disposal electric vehicles (GDEVs) integrated with deep neural networking (DNN) and intelligent transportation system (ITS) in smart city management system (SCMS). Wireless personal communications, 123(2), 1733-1752.

[9] Lin, H. H., Hsu, I. C., Lin, T. Y., Tung, L. M., & Ling, Y. (2022). After the epidemic, is the smart traffic management system a key factor in creating a green leisure and tourism environment in the move towards sustainable urban development? Sustainability, 14(7), 3762.

[10] Das, M., Tao, X., Liu, Y., & Cheng, J. C. (2022). A blockchain-based integrated document management framework for construction applications. Automation in
Construction, 133, 104001.