International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023, ISSN No: 2348-9510

BLOCKCHAIN-BASED IDENTITY VERIFICATION (DECENTRALIZED IDENTITY VERIFICATION)

Anvesh Gunuganti
maverickanvesh@gmail.com

Abstract

Blockchain has become a revolutionary concept applicable in almost all domains, among which one stands out: identity verification. This paper presents a brief insight into Blockchain-based identity verification systems and the relevance of aspiring to use them over the traditional centralized identification system approach. In its original form, Blockchain preserves the unchangeability of information and the decentralization of decision-making, allowing one to implement the concept of secure and autonomous digital identity. This paper has attempted to analyze the applicability and efficacy of the Blockchain approach to identity verification across different domains. Some areas of focus have included security, privacy, usability, or user experience, as well as compliance with set legal and regulatory frameworks. In this paper, we present the results of the mapping and data extraction phases, which involve identifying and comparing the methodologies, results, and implications of Blockchain-based ID management with in diverse domains. The integration of the results to make comprehensive conclusions indicates the possible positive impact and critical issues to be examined in implementing Blockchain-based identity verification systems. The strength of entity authentication across industries and the innovation of new Blockchain technology will enable the future of identity solutions for the stewardship of users.

Keywords - Blockchain-based identity verification, Decentralized identity management, Digital identity security.

I. INTRODUCTION

A. Overview of Blockchain Identity Verification

Blockchain was adopted primarily for digital currency systems and has since become a revolutionary tool – a platform that lies to other sectors. In its simplest form, Blockchain refers to a shared ledger that can store transaction data and is distributed across a decentralized set of computers [1]. Its simplicity and efficiency also allow for the formation of safe and clear networks of relationships without third parties being involved.

In the segment of identity verification, Blockchain is moving from the centralized types of solutions, which are quite traditional. Through employing cryptographic science and consensus algorithms, Blockchain technology addresses the problem of how best to establish a digital identity that is safe and invulnerable to tampering and, at the same time, owned and controlled by the user. Thus, identity verification on the Blockchain includes creating, controlling, and approving digital identities with the help of crypto graphic keys. Individual identification data remains the user's personal information, encrypted, stored locally, and distributed across the Blockchain [2]. Using cryptographic signatures and Blockchain technology, these individual scan encrypt their data and provide access to some information only to those with whom they want to share it.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023, ISSN No: 2348-9510

B. Importance of security and privacy

The current techniques in identity verification presume the knowledge of central storage facilities operated by governments, financial institutions, or corporations (as shown in Fig 1). Nonetheless, centralized systems have potential security risks and challenges, such as hacking, impersonation scams, and intrusion. Also, it frequently involves high-stakes decision-making that involves submitting personal profile details. Therefore, there are issues of privacy and data sovereignty.

Blockchain eliminates these vulnerabilities by using transparency and decentralization, ensuring the digital identity is self-sustaining and secure [3].Organizing identity information as decentralized records and applying complex algorithms can significantly reduce the threat level of cyber intrusion. Further, decentralized identity management systems developed using Blockchain technology provides the identity owner and actual user a right of privacy over their identification details.

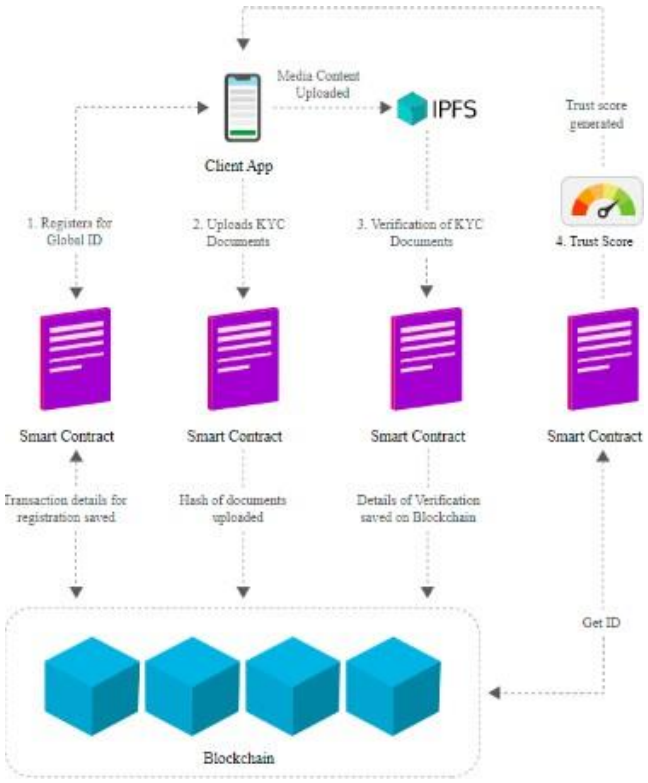

Fig1: Blockchain identity management [10]

Due to the continuous increase in the adoption and complexity of cyber attacks, the more there is the importance of safeguarding user identity verification system solutions. Blockchain technology seems to be the best solution that simultaneously increases the level of protection and leads to increased individual control over personal identification [2]. Fig 2 depicts the case of implementing Blockchain in Know Your Customer (KYC) activities. It shows the flow around identity proofing and demonstrates how Blockchain makes Customer Due Diligence secure, clear, and quicker for every verification process.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023, ISSN No: 2348-9510

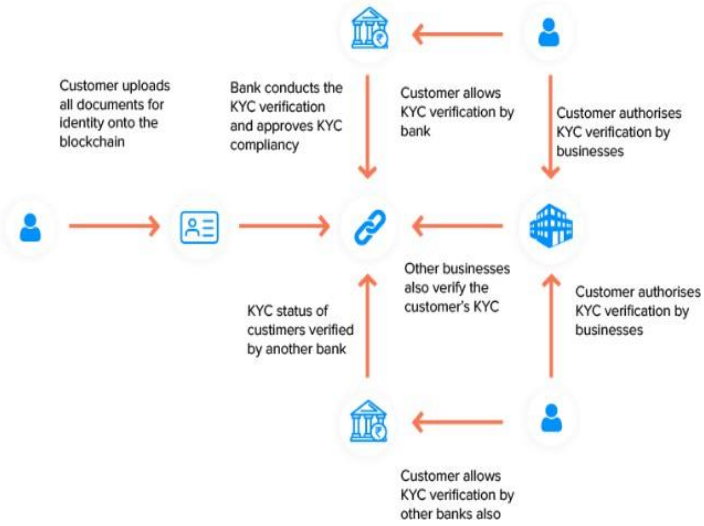

Fig2: Implementation of Blockchain[11]

C. Aim of the review: Blockchain-based identity verification

This review aims to provide a comprehensive analysis of existing research in terms of whether or not its application of Blockchain technology is effective, safe, and feasible for identification. This review will focus on the following key aspects:

1. Feasibility: The review will analyze the possibility of applying the Blockchain approach toward ID verification in the target industries and the spheres mentioned above. This can include evaluating the technology readiness and its general architectures for supporting such solutions.
2. Security: The verification process of identity is very sensitive regarding security measures. Among the areas to be covered in the review is how Blockchain boosts the security of identities by offering the protections of cryptographic, decentralized storage, and immutability [7]. Moreover, it will explore the effects of other security issues, including identity theft, data breaches, and tampering with these Blockchain systems.
3. Privacy: Security measures are always a big issue regarding identity checks, keeping in mind the highly sensitive nature of information belonging to a person. The review will also highlight the challenges facing Blockchain- based identity verification solutions and how these solutions tackle privacy and ownership by allowing users to manage their identity data in a manner that allows them to reveal identity data to the extent they deem necessary without compromising anonymity or the confidentiality of their identity data [8].
4. User Experience: One critical factor determining the level of use of any ID verification system is ease of use. The review will consider the general overall usability of the concepts and their applicability as efficient tools for individual and business needs. It entails comparing aspects such as one's ability to get on board, the procedures of authenticating oneself, and the layout of the user interfaces [9].
5. Regulatory Compliance: Ensuring that information is collected in compliance with legal and regulatory standards is crucial to identification proofing. Some industries are governed by strict norms and policies, such as the financial and healthcare industries [7]. The review will also determine how the Blockchain identity verification solutions conform with laws, regulations, and best practices when addressing issues relating to data protection, money laundering, and know your Customer, among other laws.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023, ISSN No: 2348-9510

As a result, this literature review seeks to synthesize the findings obtained from the selected academic papers and empirical studies to estimate the advantages, risks, and recommendations for implementing Blockchain technology for identity verification. Overall, it aims to further propose more effective and secure approaches to identity management for e-commerce and real-life communication.

II. METHODOLOGY

This section describes the method used to systematically review the literature on Blockchain-based identity confirmation. This includes formulating research questions, developing a search strategy, identifying databases and keywords, and establishing inclusion and exclusion criteria. Based on a careful study of the collected data, the study seeks to provide a detailed understanding of blockchain's effectiveness and applicability in identity confirmation.

When developing the research question, the PICOC framework (Population, Intervention, Comparison, Outcome, and Context) was used to define the study variables and boundaries. In more detail, it is proposed to consider the population as users of the Blockchain identity verification systems, the intervention as the application of Blockchain technology, the comparison to the traditional methods of identity verification, the outcome as the efficiency in the mitigation of security and privacy issues, and the context is the industries and segments adopting the identity verification systems. This approach helped to adequately construct our research question and provide for consideration all relative factors affecting the assessment of Blockchain technology in identity verification.

TABLE I. PICOC TABLE

Aspect	Description
Population	Users of blockchain-based identity verification systems
Intervention	Implementation of blockchain technology
Comparison	Traditional identity verification methods
Outcome	Effectiveness in addressing security and privacy concerns
Context	Various sectors and industries using identity verification systems

A. Research question

How effectively is Blockchain technology addressing security and privacy concerns in identity verification?

B. Search Strategy

The approach for selecting articles for the review will also involve using the most relevant search terms in various databases and scholarly journals and trends that are most relevant to the study. The disadvantage of using Grey literature is that it may not have been peer-reviewed and may contain outdated information, but to get an overview of the topic, both will be used. An explicit search will be conducted by entering asset of keywords; Boolean operators will also be used to get more relevant results.

The following databases will be searched:

- IEEE Xplore
- Science Direct
- Web of science Keywords:
- Blockchain
- Identity verification
- Decentralized identity
- Digital identity
- Security
- Privacy
- Authentication
- Smart contracts
- Cryptography Search String:

("Blockchain") AND ("Identity verification" OR "Digital identity") AND ("Security" OR "Privacy" OR "Authentication")

C. Inclusion and Exclusion Criteria

Inclusion Criteria:

- Articles published in peer-reviewed journals or conference proceedings.
- Publication year between 2019 to 2022.
- Open-access articles only.
- Articles written in English.
- Focus on Blockchain technology for identity verification.
- Relevance to the topic is evident in the title and abstract.

Exclusion Criteria:

- Publications outside the specified publication timeframe
- Articles without open access availability.
- Articles not written in English.
- Irrelevant to Blockchain-based identity verification as determined by title and abstract screening.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023, ISSN No: 2348-9510

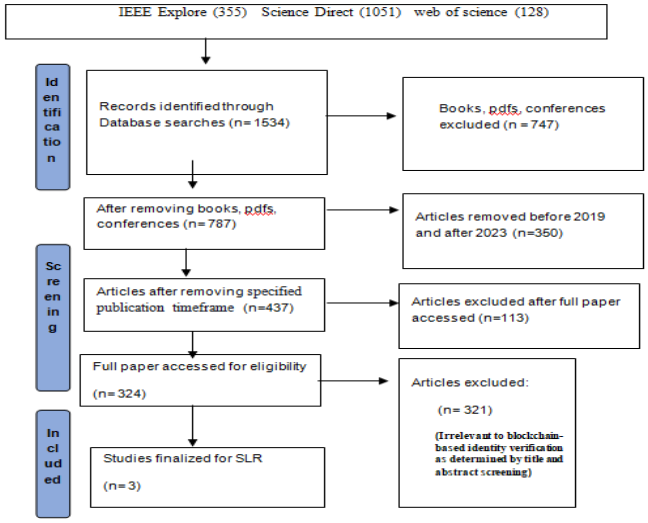

Fig 3: PRISMA Framework

D. Inclusion and Exclusion Criteria

The study [4] aims to address the human Internet of Things (IoT) privacy issues using verifiable anonymous identity management (VAIM), an identity management approach that deals with privacy issues. Though Blockchain technology offers hope to identity management systems (IDM), the very nature of the ledger system poses questions about privacy. To mitigate this, VAIM has implemented ways of creating privacy channels within the user-to-the-user communication model with the help of identity verification and an access control mechanism. Some of the valuable contributions are integrating the zero-knowledge proof (ZKP) identifiable elements protocol to promote the extent of identity unlinkability of the IDM system, integrating the blind ordered multi-signature (BOMS) protocol for effective and efficient management of transactions and their verifications, and incorporating certain specific ZKP algorithm. They further guarantee strong privacy protection and expand the use of identity management systems across the HIoT environment.

The paper [5] includes a systematic literature mapping of Identity Management (IdM) to identify how Blockchain has impacted this field by addressing some of the challenges that have ensued in the past. It can facilitate researchers to consider new trends in IdM with Blockchain, assess the applicability of Blockchain in solving IdM issues, compare different IdM frameworks in terms of security and privacy context, reveal the initiatives in block-chain IdM, explore solutions in consensus algorithms, and observe the active research works in the field of IdM with Blockchain. In synthesizing these findings, the paper supports future studies on the IM and Blockchain intersection by offering vital insights into a timely and emerging domain.

The purpose of the paper [6] is to consider the role of eHealth Identity Management (IdM) with the development of eHealth systems and the future of IdM through Distributed Ledger Technology (DLT), including Blockchain. Using the Blockchain, patients can control their identity completely, improving the reliability of the data, which is both immutable and available. The paper could be regarded as an overview of Decentralized Identity Management through Blockchain, and the paper aims to discover the prospect of developing new health identity systems based on Blockchain. It introduces identity management in eHealth environments and scenarios, explores current decentralized identity management, and discusses decentralized identity models. Furthermore, the paper will briefly explore the current state of distributed identity solutions. Based

on the cases and certain difficulties, it will analyze the problems with implementing decentralized identity management in the healthcare sector.

The paper [13] explains that centralized approaches to digital identity have profound dangers and problems. SSI, which refers to the governance of digital identities, enables people to personalize their identities in the digital world through proofing and authentications. Blockchain contributes to SSI because decentralization, security, and transparency on any data in the system can easily be achieved. Some examples of the existing SSI platforms are uPort, Sovrin, and Civic, built on the base of Blockchain, and they are not free from some drawbacks, like limited compatibility of the systems, unsatisfactory rates of scalability, and not very convenient interface. Thus, the discussed case demonstrates the opportunities and challenges of applying Blockchain technology to resolve security and privacy issues in IaaS while pointing to the directions for further studies.

E. Data Extraction and Synthesis

The process of gathering the required data includes identifying sources and analyzing essential findings of three articles provided below, all of which address the subject of Blockchain-based identity management within various domains. Firstly, from the study derived from Verifiable Anonymous Identity Management (VAIM), it is possible to obtain information regarding the method used to increase the number of identity-linked techniques with ZKP algorithms and the BOMS protocol [4]. Further, findings on the effectiveness of privacy protection and the ability to expand the application range promised by the given scheme will also be outlined.

Secondly, secondary data will be collected from the article, and sources utilizing systematic literature mapping of IdM in Blockchain will be identified. The data will be extracted regarding the research trends, challenges addressed, and the initiatives taken in this field. This is useful regarding the main and additional keywords applied, the bases and databases explored, the filters employed, and the overall number of identified studies.

From the paper on decentralized identity management using Blockchain in eHealth systems, data will be gathered on what the writers considered as the importance of eHealth Identity Management (IdM), the possibility of DLT in a decentralized identity management scenario, and the opportunities for decentralized identity management strategies in healthcare as identified in the paper. These features consist of an assessment of eHealth identity management, use cases, existing approaches to digital identity management, decentralized identity models, present decentralized identity initiatives, and difficulties in implementing decentralized identity management in healthcare [5].

Hence, integrating the data gathered from these articles will achieve a systematic understanding of the methods, conclusions, and implications of Blockchain identity management in the various domain areas. That synthesis will allow one to reveal shared concerns, new directions, and possible obstacles to further work in the discussed sphere, which is critical for further discursive and concluding considerations regarding the efficiency and relevancy of applying Blockchain-based Identified management.

III. FINDINGS AND DISCUSSION

This paper presents the state-of-the-art and known issues and challenges in Blockchain-based identity verification from the existing literature. Blockchain technology can, therefore, be described as the new way of managing identity as it fully utilizes technological advancement to make methods more decentralized, secure, and transparent. By applying the highest security measures

and hashes in the computation of consensus algorithms, Blockchain makes the construction of exclusive and safe digital identities possible for every individual.
Based on Blockchain technology, identity verification has major implications in several fields. For instance, a patient can uniquely own medical records and share them with only authorized members while the database is protected and cannot be tampered with. Likewise, in banking, the technology can be applied to KYC to cut costs and increase the security of the Know Your Customer processes due to the technology's ability to verify the customer's identity while preserving their data. These applications demonstrate the possibilities of Blockchain solutions for ID Vérification to be more effective regarding security, efficiency, and user experience while considering the user's privacy and regulation.

Technical Aspects of Blockchain Implementation
Advanced cryptographic functions like hash functions and public key cryptography provide security and correctness of the distributed ledger in the Blockchain mechanism. Each block has a header in this structure, and the header contains information about the previous block's hash code; therefore, it is very difficult to alter the data stored in the blocks in any specific chain. Public-key cryptography allows users to obtain a pair of keys, where the private key signs transactions, while the public key's purpose is to check these signatures, which means that the transactions demand authentication and non-repudiation. Such cryptographic essentials are the basis for secure management and identification verification in the Blockchain without involving a centralized authority.
Consensus algorithms play the most critical role in the decentralization of Blockchain systems. The two well-known consensus algorithms for validating transactions and adding blocks to the chain are known as Proof of Work (PoW) and Proof of Stake (PoS). PoW requires miners to complete unique problems, which are mathematical computations, to authenticate the possible transaction and give stronger security to the network against hackers to control the network and achieve consensus of all individuals in the network. On the other hand, PoS chooses the validators according to the amount of the cryptocurrency they possess and are willing to "lock" or use in staking, thus being more energy-efficient compared to PoW while at the same time maintaining the network's security.

Smart Contracts and Decentralized Applications (DApps)
Smart contracts can be described as self-executing applications containing the contract's business logic that will implement terms by automatically executing or verifying contractual clauses based on transactions recorded on a Blockchain. Such a contract allows the DApps to handle identity verification relatively independently, hence improving the efficiency and transparency of the identity management process. By removing middlemen in identity verifications, smart contracts provide safer and more efficient means of undertaking identity checks, improving users' confidence in computerized engagements.

Comparison with Traditional Methods and Emerging Challenges
In many cases, the identification methods allow for security holes and violations of subjects' privacy rights. These problems are solved identically to the solutions inherent to Blockchain technology, ensuring decentralization with cryptographic techniques and the concept of the pseudonymity of the users. Thus, the present use of Blockchain solutions in identity verification remains problematic due to problems like scalability, compliance, and cross-chain compatibility. Mitigating these factors will be important in achieving the optimum use of Blockchain technology to change the face of identity management across various sectors.

International Journal of Core Engineering & Management
Volume-7, Issue-07, 2023, ISSN No: 2348-9510

Management of identities in eHealth systems is quite suitable for decentralization, which can significantly contribute to patient data protection and availability (as shown in Fig 4). Through the use of Blockchain, patients would have control of their data in a way that has not previously been possible while at the same time guaranteeing consistency and accessibility [5].

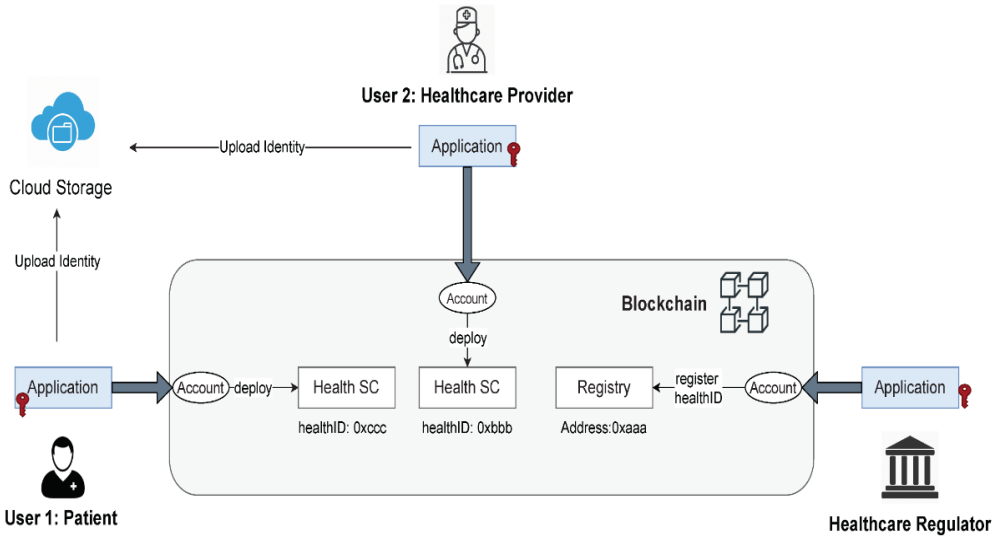

Fig 4: Healthcare identity management system [12]

From the selected articles, it is possible to develop the experience of carrying out further work to adopt Blockchain-based identity verification systems, as well as their advantages and potential problems. The features that other similar applications share can be rated as common and may include the following: security, privacy, compliance with regulations and requirements, and usability. However, further studies and advancements are still required about the possibility of applications that can scale effectively, regulatory and legal questions, and the ability to work across networks.

In conclusion, it is important to note that using Blockchain-based solutions for identity verification is a promising avenue to redefine identity management across different sectors in the coming years. Considering relevant security and privacy issues, data quality improvement and increased user control in identity management brought by future Blockchain-based frameworks can help develop safer, effective, client-oriented identity verification processes.

A. Answers to research question

The selected articles help answer the research question, 'How well does Blockchain technology perform in solving security and privacy concerns in identity verification?' While each article provides information on a different aspect of Blockchain-based identity verification systems, they all cover all the aspects necessary to properly evaluate the technology.

Verifiable Anonymous Identity Management (VAIM): This work unveils myriad issues regarding identity management on the Blockchain, introducing innovative solutions that promote security and privacy using cryptographic innovations. Using ZKP, specifically the BOMS protocol, ensures that identity information remains deviously linked and anonymous, eliminating the instances and possibilities of identity theft and unauthorized access to sensitive data. This article also demonstrates how Blockchain can provide reliable security for privacy, a fascinating aspect of the research question [4].

Systematic Literature Mapping of Identity Management (IdM) in Blockchain: While this article represents a high-level review of an extensive area of study, it can be seen that Blockchain-based identity management systems are still in their infancy. As a result, besides focusing on several prospects and trends, challenges, and directions, it reveals how Blockchain technology meets and responds to the security and privacy issues that might occur in various settings. From the considered study, it is possible to define such general tendencies as the need to develop cryptographic protection, widespread decentralized storage, and user-oriented solutions for increasing security and personal data protection during the ID check. This mapping also highlights the general understanding of the ability of Blockchain to ensure security, as market players acknowledge.

Decentralized Identity Management in eHealth Systems: This paper aims to evaluate the practical benefits and uses of Blockchain technology in the healthcare industry, particularly in decentralized identity management related to patients' records security and privacy [6]. It elucidates how Blockchain empowers patients to own their health data and how patient data is protected from tampering and hoaxes. It also highlights the challenges of implementing decentralized solutions within centralized environments and meeting regulations. The knowledge described in this article enriches the understanding of practical concerns and the benefits of applying Blockchain in the most critical domain framework, underscoring the research question's relevance.

IV. CONCLUSION AND FUTURE DIRECTION

Overcoming these hurdles calls for better implementation strategies considering the technical, financial, regulatory, and user stances. In this way, leaders and managers of different organizations should effectively address the mentioned challenges to adopt Blockchain-based identity systems, which enable organizations to improve identity verification and security, increase transparency, and optimize organizational processes.

The proposed concept for effective digital identity management based on Blockchain will help overcome the adverse effects of applying IDMS. Implementing the Blockchain structure, properly using the cryptographic technique, and embracing user-centered design principles improve security, privacy, and ownership over personal information. The nature of the current studies and trends' analysis shows the efficiency and real-world implementation of Blockchain in identifying various industries. Still, numerous problems exist scaling, compliance with local requirements, and more issues with application interfaces. Dealing with these issues requires thinking about multi-stakeholder initiatives of governments, the private sector, and academia to achieve the potential of Blockchain ID verification systems. Therefore, future work in the field is expected to be directed toward enhancing the categorization of privacy-maintaining mechanisms, the growth of the efficiency of the solutions being implemented, and the integration of new protocols that would improve the functionalities of Blockchain in developing the concept of the new digital identity paradigm. Blockchain has the potential to create an innovative and effective foundation for security, transparency, and all-embracing collaboration.

Research Question and Hypothesis: In what ways can blockchain identity verification solutions maximize scalability and, at the same time, optimize security? A hypothesis that may be made here is that sharding protocols will greatly improve the scalability of the Blockchain networks if adopted, with strong security measures also incorporated to ensure that identity verifications are effective even during heightened traffic.

Future Research Directions: Various enhancements, including privacy-preserving measures, scalability solutions such as sharding, and interoperability standards, are expected to unlock Blockchain-based identity verification systems to a level beyond the current state. The following directions could be researched further: the impact of increased privacy levels on trust and usage rate, the effectiveness of new consensus algorithms when protecting transaction data, and the practicality of forming global standards for frictionless identity checks across project platforms. Building on these areas will also help to add to blockchain technologies' dynamic developments and improvements in identifying different forms of transitional environments. In conclusion, utilizing the blockchain-based mechanism in identity verification presents great potential for deep transformations in this contemporary domain and for defining the future of more effective and less centralized approaches to managing identities in the digital world. Based on the study's findings, Blockchain technology can still shape the future of the Internet through research, collaboration, and innovation to provide a secure, more transparent, and inclusive Internet system.

Implementation Challenges of Blockchain-Based Identity Systems

The use of Blockchain identity systems in real-environment processes also provokes several usable issues that need to be conditioned to ensure the correct application of the system.

- **Cost Considerations:** These are costs incurred at the beginning of the network establishment to implement the Blockchain solution, the expansion of the Blockchain network, and other costs that may be incurred in the future for the maintenance of the solution. The costs of creating new Blockchains and developing smart contracts go into the overall implementation costs.
- **Integration with Existing Systems:** Existing IT assets present some issues because of IT compatibility. The data integration process must be further facilitated through a shared database with other systems to promote weak crossover with the external environment. Blockchain networks need to interface successfully with other systems.
- **Regulatory and Compliance:** GDPR is a type of legislation that specifies the handling of personal data. Thus, it is crucial to introduce proper methods to properly work with data in Blockchain. Compliance with KYC/AML, on the one hand, while promoting user privacy, is a major factor that increases the difficulty with implementations.
- **Scalability and Performance:** Maximizing the possibilities of Blockchain networks for IDV in terms of the number of transactions is crucial. Ensuring a large number of transactions per time, small transaction response time, and fair use of system resources are some of the key goals that, if not met, reduce system performance.
- **User Adoption and Usability:** The education of users on decentralized identity solutions is very important to increase their adoption. Usability testing and, more often, feedback are key in bringing about the best interfaces and the overall experience of an application.

REFERENCES

1. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare," Healthcare, vol. 9, no. 6, p. 712, Jun. 2021, doi: https://doi.org/10.3390/healthcare9060712.
2. Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M.-A. Fatima, "Blockchain-Based Identity Verification System," 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET), Oct. 2019, doi: https://doi.org/10.1109/icsengt.2019.8906403.
3. Malik, K. Parasrampuria, S. P. Reddy, and S. Shah, "Blockchain Based Identity Verification Model," IEEE Xplore, Mar. 01, 2019. https://ieeexplore.ieee.org/document/8899569
4. . Ra, T. Kim, and I. Lee, "VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things," IEEE Access, vol. 9, pp. 75945–75960, 2021, doi: https://doi.org/10.1109/access.2021.3080329.
5. T. Rathee and P. Singh, "A Systematic Literature Mapping on Secure Identity Management using Blockchain Technology," Journal of King Saud University - Computer and Information Sciences, Mar. 2021, doi: https://doi.org/10.1016/j.jksuci.2021.03.005.
6. M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective," Sensors (Basel, Switzerland), vol. 20, no. 2, p. 483, Jan. 2020, doi: https://doi.org/10.3390/s20020483.
7. E. Bandara et al., "Casper: a Blockchain-based system for efficient and secure customer credential verification," Journal of Banking and Financial Technology, Dec. 2021, doi: https://doi.org/10.1007/s42786-021-00036-3.
8. Nusantoro, R. Supriati, N. Azizah, N. P. Lestari Santoso, and S. Maulana, "Blockchain Based Authentication for Identity Management," IEEE Xplore, Sep. 01, 2021. https://ieeexplore.ieee.org/abstract/document/9589001
9. Z. Zhong and Y. Liu, "A Blockchain based Identity Management System Considering Reputation," Sep. 2019, doi: https://doi.org/10.1109/iciscae48440.2019.221582.
10. "Benefits of Blockchain in Identity Management - Rejolut." https://rejolut.com/blog/Blockchain-in-identity-management/
11. Camarda, "Compliance Strategies for Blockchain-Based Identity Management Solutions," Identity Defined Security Alliance. https://www.idsalliance.org/blog/compliance-strategies-for-Blockchain-based-identity-management-solutions/
12. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-ID: A Blockchain-Based Decentralized Identity Management for Remote Healthcare," Healthcare, vol. 9, no. 6, p. 712, Jun. 2021, doi: https://doi.org/10.3390/healthcare9060712.
13. K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Sep. 2020, doi: https://doi.org/10.1109/brains49436.2020.9223312

ACRONYMS

- HIoT: Human Internet of Things
- VAIM: Verifiable Anonymous Identity Management
- IDM: Identity Management System
- ZKP: Zero-Knowledge Proof
- BOMS: Blind Ordered Multi-Signature
- DLT: Distributed Ledger Technology
- KYC: Know your customer