A Survey On Blockchain Identity Authentication System

Azim Baji Krishna
Department of Computer Engineering
Pillai College of Engineering
New Panvel, India
azimbaji19@gmail.com

Ramkrishna Sarvesh Mourya
Department of Computer Engineering
Pillai College of Engineering
New Panvel, India
ram23052002@gmail.com

Amulya Manoj Walimbe
Department of Computer Engineering
Pillai College of Engineering
New Panvel, India
amulyawalimbe02@gmail.com

Sakshi Brijesh Singh
Department of Computer Engineering
Pillai College of Engineering
New Panvel, India
singhsakshi072002@gmail.com

Sangeetha Selvan
Depaertment of Computer Engineering
Pillai College of Engineering
New Panvel, India
sangeethas@mes.ac.in

***Abstract*—** The development of blockchain technology has opened up new avenues for creative approaches to authentication and identity management. The information from several research reviews on blockchain-based identity management and verification is summarised here. Scholars have investigated the possibility of blockchain technology to transform conventional identity verification techniques by utilising attributes like immutability, transparency, and decentralised consensus. The studies emphasise that for blockchain-based identity systems to be widely used, safe key management, standardisation, and trustworthy stakeholders are essential. On the blockchain, smart contracts are essential for guaranteeing the accuracy of user data and creating legitimate identities. Furthermore, the efficiency and security of identity management systems are improved by the combination of consortium-oriented blockchain networks with biometric authentication. The study emphasises how important decentralised, transparent, and safe blockchain technology is for protecting user information and workflows. Blockchain-based identity verification systems present a viable way to fight identity theft and fraud in the digital sphere by solving issues with verification procedures, privacy risks, and centralised structures.

Keywords- Blockchain, Authentication, Transparency, Decentralised, Privacy.

I. INTRODUCTION

The landscape of identity management and authentication is undergoing a paradigm shift with the emergence of blockchain technology. The research highlights the decentralised, transparent, and secure characteristics of blockchain technology, which makes it a prime contender to transform conventional identity authentication techniques. Utilising the immutability and consensus processes of blockchain technology, entities may create strong identity verification frameworks that put user privacy and data security first. Three major themes that have been covered in the literature include the use of biometric authentication to strengthen system integrity, the development of self-sovereign identity models, and the incorporation of smart contracts for on-chain verification. In addition, the study highlights that user-centric strategies, standardised protocols, and regulatory compliance are necessary to guarantee the efficacy and scalability of blockchain-based identity systems. Blockchain technology develops as a disruptive force that may both empower individuals with greater control over their personal data and mitigate the risks associated with identity theft and fraud, as industries navigate the complexity of digital identity management.

II. LITERATURE SURVEY

Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey [1]

The paper titled “Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey” proposed by Md. Rayhan Ahmed presents a comprehensive survey of blockchain-based identity management systems (IDMS) and self-sovereign identity (SSI) ecosystems. It assesses academic and commercial offerings within the domains of IoT, cloud computing, EMH and WSN. The paper delineates crucial elements of blockchain-basedw Identity Management Systems (IDMS) and evaluates academic solutions in terms of simplicity, trust, and integrity. A comprehensive security analysis is conducted, encompassing diverse attack types and corresponding mitigation strategies. The document extensively explores challenges, issues, and potential avenues for future research. Additionally, it compares the resilience of proposed solutions in blockchain against common attack types.

Integrated identity and auditing management using blockchain mechanism [2]

The paper titled "Integrated Identity and Auditing Management Using Blockchain Mechanism" proposed by Prashant Madhukar Yawalkar delves into the establishment of a framework reliant on blockchain technology designed for federated identification and

auditing. It offers an overview of relevant research in the realm of blockchain identity management, emphasizing the decentralized, secure, and transparent nature of blockchain technology that renders it suitable for identity management systems. Notably, major corporations such as Microsoft, Accenture, and Oracle have acknowledged the advantages of employing blockchain for safeguarding client IDs. The review outlines various blockchain-based identity management platforms, including Sovrin, ShoCard and uPort. These platforms furnish open and verifiable blockchain identities, enabling users to access their identifying attributes from credible third-party sources. The paper underscores the distinction of the proposed framework from these platforms by conducting identity verification within the blockchain itself, thereby ensuring the security of user data and processes.

Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior [3]

The literature review of the paper "Digital Identity Verification and Management System of Blockchain-blockBased Verifiable Certificate with the Privacy Protection of Identity and Behavior" proposed by Zhiming Song explores existing blockchain-based digital identity verification and management systems (DIVMSs) and related techniques. The authors provide an overview of three main architectures found in DIVMSs and discuss various systems proposed within each architecture. The analysis emphasizes the integration of smart contracts for on-chain verification of identity, underscoring the benefits of self-sovereign identity control and the scalability ingrained in blockchain-driven DIVMSs. Additionally, it acknowledges the drawbacks of conventional DIVMSs, particularly concerning privacy protection.

Towards Using Blockchain Technology To Prevent Diploma Fraud [5]

The paper “Towards Using Blockchain Technology to Prevent Diploma Fraud” proposed by Qiang Tang discusses the use of blockchain technology to prevent diploma fraud in the education and training sector. The authors present a generic framework for digitized diploma management systems, detailing functional and non-functional criteria. They observe a deficiency in existing blockchain-based systems in meeting these criteria. In response, they propose a blockchain-facilitated solution using basic cryptographic primitives and data structures. Their investigation affirms that the proposed solution inherently satisfies identified requirements and has room for further improvements to strengthen security and privacy features. Finally, they assess the computational complexity of the proposed solution, demonstrating its practical feasibility.

A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain [6]

The paper titled “A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain” proposed by Sheng Gao encompasses a comprehensive review of traditional identity management solutions, federated identity management, and privacy-preserving authentication schemes. The paper explores blockchain integration into identity authentication, focusing on IoT and healthcare. It critiques centralized systems, proposing blockchain for user-controlled identity management, ensuring privacy and reducing storage overhead. Cryptographic techniques like ECDSA and RSA enhance communication security. Emphasizes sca la bility, communication security, and cross-blockchain authentication. Evaluates security and performance, confirming feasibility and meeting security standards.

Decentralized and Self-Sovereign Identity: Systematic Mapping Study. [7]

The paper titled “Decentralized and Self-Sovereign Identity: Systematic Mapping Study” proposed by ŠPELA ČUČKO is a systematic mapping study that aims to provide a comprehensive overview of decentralized and Self-Sovereign Identity (SSI) research. The process encompasses the collection, examination, and categorization of research papers according to their contributions, application domains, IT sectors, research types, methods, and publication venues. The research reveals a notable increase in the volume of published papers over the years, predominantly found in conference proceedings. Following the screening phase, 120 studies were selected for the final analysis. A classification framework was developed based on essential concepts derived from paper titles, keywords, and abstracts. The study also scrutinizes trends, challenges, demographics, and gaps within the decentralized and SSI field. The methodology involves formula ting research questions, devising a search strategy, screening papers, keywording, creating a classification framework, and extracting, classifying, and mapping study data.

Blockchain-Based Identity Verification System [9]

The paper “Blockchain-Based Identity Verification System” is proposed by Arshad Jamal. The decentralized system, akin to the blockchain concept, enables registered individuals to access personal records. This system caters to three main users: the user, authority, and third-party. Users can grant third-parties access to their data and view a list of requesters. Authorities are empowered to upload user records on the blockchain and authenticate companies seeking requester registration. Third-parties can request access to user data. The system employs blockchain security features, ensuring transparency regarding data access. The paper underscores the significance of blockchain identity in empowering society to take control of their personal information.

Blockchain-Based Identity Verification Model [10]

In this paper, “Blockchain-Based Identity Verification Model” the author Gunit Malik has suggest a blockchain-driven approach to validate the legitimacy of documents issued by Indian government entities. The existing

procedure for issuing and authenticating identification documents is characterized by inefficiency and prolonged processing t imes. The envisioned model seeks to enhance both efficiency and security. The solution utilizes a private permissioned blockchain network to facilitate the seamless exchange of authenticated government documents among government entities and private organizations, eliminating the necessity for manual intervention. The benefits of this system encompass rapid, dependable, and secure document verification, along with decreased expenses and environmental impact.

Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective. [11]

The paper titled "Blockchain-Based Identity Management: A Survey from the Enterprise and Ecosystem Perspective" proposed by Michael Kuperberg provides a comprehensive analysis of blockchain-based identity management solutions, covering topics including existing identity standards, strategic IT planning for privacy laws, and decentralized identity solutions like self-sovereign identity. It evaluates 43 blockchain-based identity solutions, comparing them with existing offerings. Evaluation criteria are defined to assess new identity management approaches. Government standards, joint ventures, and market forces in IAM are discussed.

Blockchain-Based Identity Authentication and Intelligent Credit Reporting [12]

In this paper titled "Blockchain-Based Identity Authentication and Intelligent Credit Reporting" method proposed by Xingxiong Zhu for financial services, e-commerce, and energy applications. The system employs multifaceted authentication, calculates weighted scores, and establishes security thresholds to enhance dynamic identity security. The utilization of distributed ledgers, smart contracts, and encryption algorithms guarantees the integrity and privacy of data. The system integrates user behavior analysis for real-time risk identification and prevention. It addresses the challenge of scarce diverse credit information from multiple dimensions by leveraging the capabilities offered by blockchain technology. Security is bolstered through the incorporation of biometrics, behavioral recognition, and cryptographic algorithms. User attribute details are safely recorded within the blockchain with generated keys. The authentication process involves comprehensive weighted average scores, managed by smart contracts to assess and mitigate risks. Additionally, artificial intelligence is employed to verify user behavior.

Analysis of Identity Management Systems Using Blockchain Technology [13]

The paper titled "Analysis of Identity Management Systems Using Blockchain Technology" proposed by Samia El Haddouti conducts an examination of three well-known Identity Management Systems employing Blockchain technology, namely Sovrin, ShoCard, and uPort. The assessment is grounded in Cameron's seven laws of digital identity, encompassing aspects like human integration, justifiable parties, directed identity, minimal disclosure, and user control. The study highlights the absence of comprehensive comprehension regarding user experience components and the difficulties associated with maintaining privacy in the context of Blockchain-based identity management. It further delves into the evolving regulatory environment concerning the storage of personal data and advocates for a more uniform approach to identity management to tackle privacy apprehensions. The document uses a systematic approach to analyze the technical details and properties of each system, providing a comprehensive overview of their architectures and functionalities. It also discusses the evolution of digital identity models and the emergence of self-sovereign identity, as well as the overview of Blockchain technology and its implications for industries.

A Comprehensive Integration of National Identity with Blockchain Technology [16]

The paper titled "A Comprehensive Integration of National Identity with Blockchain Technology" proposed by Kumaresan Mudliar presents the integration of blockchain technology with national identity, creating a hierarchical system where only sanctioned officials can access individual information. The system utilizes Aadhar, a unique-identity number issued to Indian citizens, and Ethereum nodes to create a decentralized, secure, and transparent national identity system. It outlines the methodology, including setting up Ethereum nodes, creating smart contracts, and developing distributed applications. The proposed model envisions applications in banking, healthcare, digital voting, and distributed cloud storage. It also discusses the potential of blockchain technology in revolutionizing economic and social infrastructure. The document accentuates the decentralized configuration of blockchain systems, the clarity ensured by pseudonymity, and the indelible nature of recorded information. It also touches upon the future scope of blockchain technology and the potential applications of smart contracts in automating approval workflows and trade clearing and settlement processes.

Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey [17]

The paper "Blockchain Technology the Identity Management and Authentication Service Disruptor: A Survey" proposed by Shu Yun Lim provides a comprehensive overview of blockchain-based identity management and authentication solutions from 2014 to 2018. The paper examines traditional identity management challenges like data breaches and proposes blockchain solutions such as Sovrin, MyData, and Waypoint. These solutions decentralize identity management for enhanced security. Various platforms like Ethereum, Hyperledger, and Bitcoin are compared for their consensus algorithms and scalability. Blockchain's potential to transform identity management is underscored, offering a holistic view of existing blockchain-based solutions in this field.

Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging. [18]

The paper titled "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging" proposed by Zhixong Chen explores the use of blockchain technology to create a Personal Archive Service System (PASS) for managing digital artifacts and identification information. It introduces the concept of Personal Digital Artifacts (PDAs) and outlines the roles of "subject," "certifier," "inquisitor," and "client" in the verification process. The system leverages blockchain features such as immutability, transparency, anonymity, and decentralized consensus. It addresses challenges in verification processes, privacy threats, and centralized models. The paper emphasizes the importance of standardization, reputable stakeholders, and secure key management for wide adoption. It also discusses the application of biometric authentication and the use of consortium-oriented blockchain networks. The PASS system aims to provide a secure, transparent, and decentralized platform for managing personal portfolios and identification information. The paper provides a comprehensive framework for leveraging blockchain technology to build a secure and efficient personal archive management system.

An Identity Management System Based On Blockchain [19]

This paper "Identity Management System Based on Blockchain Technology" is proposed by Yuan Liu. The system integrates identity authentication and reputation management to create an individual online reputation data file within blockchain blocks. Smart contracts are utilized to ensure the reliability of user information, while binding the user's entity information to the public key address establishes the authentic identity of a virtual user on the blockchain. A token represents the reputation, proving to be an effective model as system participants are inclined to uphold and manage their personal reputation. The paper explores the merits of blockchain technology, a secure and tamper-resistant distributed database system. The architectural structure of interconnected blocks in a chain, linked through cryptographic hash, offers robust distributed security. Additionally, the paper delves into Ethereum and Smart Contracts, defining the latter as a computer-program-controlled, numerically defined contract specifying participants, execution conditions, and transaction rules in detail. Unlike traditional contracts, smart contracts are entirely governed by computer programs and operate independently of any central authority.

Blockchain-based System for Secure Data Storage with Private Keyword Search [20]

The paper titled "Blockchain-based System for Secure Data Storage with Private Keyword Search" proposed by Hoang Giang Do presents a system called BlockDS, which leverages blockchain technology to provide secure distributed data storage with private keyword search. The system comprises Distributed Encrypted Data Storage, Anonymous Access Control, and Private Keyword Search. Data owners can encrypt and outsource data to a federated cloud, with blockchain nodes maintaining encrypted keyword tags for access. It ensures data integrity through distributed proof-of-retrievability and grants anonymous access control. Private Keyword Search enables specific data identification without full dataset downloads. Client-side encryption and distributed storage across peer nodes are employed. Off-chain distributed hash table access is facilitated via blockchain. Cryptographic techniques support keyword search and access control.

Decentralizing Privacy: Using Blockchain to Protect Personal Data [21]

The paper titled "Decentralizing Privacy: Using Blockchain to Protect Personal Data" proposed by Guy Zyskind presents a decentralized personal data management system that utilizes blockchain technology to address privacy concerns. The paper integrates blockchain and off-blockchain storage to prioritize privacy and trust. It addresses concerns over centralized data collection and user privacy. Advocates for a decentralized model empowering users to control their data. The platform utilizes blockchain as an access-control manager for secure data handling. Technical details include network protocols and cryptographic elements.

Identity Verification System Using Data Hiding and Fingerprint Recognition [22]

The literature review discusses, "Identity Verification System Using Data Hiding and Fingerprint Recognition" proposed by Guorong Xuan to ensure secure online transactions. The system involves encrypting and embedding the client's account information into their fingerprint image via data hiding, subsequently the information is transmitted to the bank through the internet. On the bank's end, the client's account details are extracted and employed to fetch the client's stored fingerprint from a centralized database. This stored fingerprint is then compared with the extracted fingerprint using fingerprint recognition technology to authenticate the user's identity. This approach proves to be more dependable and secure compared to relying solely on password transfers.

TABLE I: Summary Table

Author Year [Citation]	Techniques	Results	Research Gaps
Md. Rayhan Ahmed 2022 [1]	Analysis of blockchain-based identity management systems (IDMS) platforms, evaluation of technical features.	A comprehensive overview and analysis of blockchain-based identity management systems (IDMS) and self-sovereign identity (SSI) ecosystems, including major platforms, technical features, emerging solutions.	The need for further analysis of emerging blockchain-based IDMS platforms, such as LifeID, UniquID, EverID, SelfKey, IDchainz, and Jolocom, Sora, to understand their effectiveness, limitations, and potential for adoption in different contexts.
Prashant Madhukar Yawalkar 2022 [2]	Conducting identity verification within the blockchain.	The development of a blockchain-based framework for identification and auditing, offering enhanced security and user data protection through identity verification within the blockchain itself.	Scalability is a major challenge in public blockchain networks like Bitcoin and Ethereum, as they necessitate validation of every transaction by all fully participating nodes.
Zhiming Song 2022 [3]	Smart contracts, self-sovereign identity management, zkSNARKs for privacy protection, and referencing relevant regulations.	A comprehensive overview of existing research and systems in the realm of digital identity verification and management systems (DIVMSs) based on blockchain is discussed, highlighting the significance of safeguarding privacy and exploring the potential of zkSNARKs to address such concerns.	The high cost of deploying the system on the public Ethereum blockchain limits its suitability, making it more suitable for private or allied Ethereum blockchains
Qiang Tang 2021 [4]	Evaluating computational performance through cryptographic algorithms and smart contracts.	Blockchain-facilitated diploma management solution that meets functional, security, and privacy requirements.	The lack of a comprehensive modeling of digitized diploma management, particularly in addressing security and privacy requirements systematically.
Sheng Gao 2021 [5]	Blockchain Technology, Public Key Infrastructure (PKI), Smart Contracts, Cryptography Methods, Consensus Mechanism.	The system enables users to generate, manage, and authenticate identity information independently via blockchain, ensuring security, privacy, and scalability.	The lack of discussion on potential vulnerabilities in the proposed blockchain-based identity authentication scheme, leaving it potentially exposed to unaddressed security risks.
ŠPELA ČUČKO 2021 [6]	Paper Screening, Classification Scheme, Data Extraction and Categorization, Result Visualization, Classification Maps,	The system provides insights into the growth, distribution, and trends of publications, as well as identifies challenges, and potential avenues for future research.	The inadequate attention given to user experience (UX) and usability in decentralized identity systems, coupled with the scarcity of research addressing well-defined architecture and patterns within this domain.
Arshad Jamal 2019 [7]	Blockchain technology, Agile Unified Process (AUP), Unified Modeling Language (UML) diagrams for system design, and system and acceptance testing for validation.	The system enhances personal data control through a decentralized blockchain-based identity verification system, facilitating secure data access and increasing trust in the reliability of personal information.	Granting personal record access poses security risks, and managing complexity and scalability may be challenging with evolving system features.
Gunit Malik 2019 [8]	Private permissioned blockchain network, Hyperledger platform, integrating direct access to document databases.	The proposed blockchain-based identity verification model offers quick, reliable, and secure document verification, leading to improved efficiency and security in the issuance and verification of government documents.	Limited scope in individual identity verification and technical complexity with various technology requirements may hinder adoption.
Michael Kuperberg 2019 [9]	Compares blockchain identity solutions, evaluating against standards, laws, and market trends	Survey of technologies for blockchain-based identity management, encompassing a comprehensive array of requirements that span ecosystem aspects, mobility and end-user functionality.	Lack of quantitative research on performance and overhead for identity management solutions based on Distributed Ledger Technologies (DLTs)

Xingxiong Zhu 2019 [10]	Integrating biometrics, behavioral feature recognition, cryptography algorithms, multidimensional authentication, security thresholds, distributed ledgers, smart contracts, encryption algorithms.	Enhanced security and privacy protection in identity authentication and credit reporting through the integration of blockchain technology.	Limited discussion on scalability and real-world implementation challenges.
Samia El Haddouti 2019 [11]	Comparative analysis and evaluation of blockchain-based identity systems (uPort, Sovrin, ShoCard)	There is a need for endeavors to establish a more uniform perspective on Identity Management to safeguard privacy when employing Blockchain.	Insufficient comprehension of contextual elements in user experience and the necessity for a more cohesive approach to Identity Management to uphold privacy when Blockchain is utilized.
Kumaresan Mudliar 2018 [12]	Ethereum nodes, smart contracts, developing distributed applications.	The hierarchical system integrating blockchain with national identity, aiming for transparency and secure access to individual information across sectors such as banking, healthcare, and digital voting.	The lack of detailed consult on potential challenges or limitations, particularly regarding the practical implementation and scalability of integrating blockchain technology with national identity systems.
Shu Yun Lim 2018 [13]	Critical survey approach to explore blockchain-based identity management and authentication frameworks.	The system offers disruptive and secure identity management, using blockchain for decentralized, tamper-proof authentication, benefiting both service providers and users.	The insufficient attention to personal privacy concerns, legislation issues, and the integration of blockchain with existing identity authentication systems for market acceptance.
Zhixong Chen 2017 [14]	Biometric Authentication, Consortium Blockchain, Smart Contracts, Verification Process, Delegated Proof of Stake (DPoS).	The Personal Archive Service System (PASS) is a decentralized, transparent, immutable, and secure personal archive management and service system that allows individuals to control and release their Personal Digital Artifacts (PDAs) while ensuring privacy and accuracy.	The need for a secure system for managing personal portfolios and identification information, as well as the development of a framework for leveraging blockchain technology to build a secure and efficient personal archive management system.
Yuan Liu 2017 [15]	Blockchain technology, smart contracts, tokenization, cryptography hashing, and crowdsourcing tasks with binary choices.	The system effectively combines identity authentication and reputation management using blockchain technology, ensuring reliability, security, and transparency in managing personal online reputation data.	Scalability challenges in blockchain systems can lead to slower transactions and higher costs as user numbers grow.
Hoang Giang Do 2017 [16]	Private Keyword Search, Anonymous Access Control, Distributed Encrypted Data Storage.	A secure distributed data storage platform with private keyword search capability, leveraging blockchain technology for data integrity and access control.	Need to address more complex requirements such as credential revocation and boolean keyword search, which are not fully covered in the current proposed system.
Guy Zyskind 2015 [17]	Repurposing blockchain into an automated access-control manager, combining blockchain and off-blockchain storage, and conducting privacy and security analysis of the system.	A decentralized system utilizing blockchain technology to enable users to securely own and manage their personal data, eliminating the dependence on third-party trust.	Need for further exploration and validation of the proposed blockchain-based solution's effectiveness in addressing privacy concerns and empowering users to control their personal data without compromising security.
Guorong Xuan 2005 [18]	Data hiding, fingerprint recognition, Quantization Index Modulation (QIM) based watermarking, JPEG 2000 coding, and performance analysis.	The proposed system achieves faster verification and secure identity verification for online transactions using a Quantization Index Modulation (QIM) based data hiding algorithm, resulting in larger embedding payload and successful watermark recovery with compressed fingerprint images.	Reduced security and hardware requirements may limit system adoption and pose risks in critical data scenarios.

III. Conclusion

In summary, identity management systems combined with blockchain technology offer a revolutionary way to overcome the problems caused by conventional authentication techniques. After analysing a wide range of literature surveys, it is clear that blockchain-based identity authentication solutions provide a reliable, safe, and user-friendly method of protecting digital identities. Through the decentralisation of governance, the improvement of transparency, and the prioritisation of privacy, these systems tackle significant weaknesses in current frameworks and establish a more robust and reliable authentication environment. The dependability and integrity of identity verification procedures on the blockchain are further strengthened by the integration of smart contracts, biometric authentication, and self-sovereign identity models. The use of blockchain technology stands out as a disruptive force that can boost user confidence in online transactions, guard against identity theft, and give users more control over their personal data as businesses and individuals navigate the constantly changing world of digital identity. Going forward, achieving the full potential of blockchain-based identity authentication systems and guaranteeing their smooth incorporation into various industry sectors will require ongoing research, standardization initiatives, and regulatory alignment.

References

[1] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ACCESS.2022.3216643

[2] Yawalkar, P. M., Paithankar, D. N., Pabale, A. R., Kolhe, R. V., & William, P. (2023). Integrated Identity and Auditing Management Using Blockchain Mechanism. Measurement: Sensors, 100732. doi:10.1016/j.measen.2023.100732.

[3] Zhiming Song, Guiwen Wang, Yimin Yu, and Taowei Chen, "Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior," Hindawi Security and Communication Networks, Volume 2022, Article ID 6800938.

[4] Shobanadevi, A., et al. "Novel identity management system using smart blockchain technology." International Journal of System Assurance Engineering and Management 13.Suppl 1 (2022): 496-505.

[5] Q. Tang, "Towards Using Blockchain Technology to Prevent Diploma Fraud," in IEEE Access, vol. 9, pp. 168678-168688, 2021, doi: 10.1109/ACCESS.2021.3137901.

[6] Gao, Sheng, et al. "A privacy-preserving identity authentication scheme based on the blockchain." Security and Communication Networks 2021 (2021): 1-10.

[7] Š. Čučko and M. Turkanović, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," in IEEE Access, vol. 9, pp. 139009-139027, 2021, doi: 10.1109/ACCESS.2021.3117588.

[8] Panait, Andreea-Elena, Ruxandra F. Olimid, and Alin Stefanescu. "Identity Management on Blockchain--Privacy and Security Aspects." arXiv preprint arXiv:2004.13107 (2020).

[9] A. 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), Shah Alam, Malaysia, 2019, pp. 253-257, doi: 10.1109/ICSEngT.2019.8906403.

[10] G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, "Blockchain Based Identity Verification Model," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899569.

[11] Kuperberg, Michael. "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective." IEEE Transactions on Engineering Management 67.4 (2019): 1008-1027.

[12] Zhu, Xingxiong. "Blockchain-based identity authentication and intelligent Credit reporting." Journal of Physics: Conference Series. Vol. 1437. No. 1. IOP Publishing, 2020.

[13] S. E. Haddouti and M. D. Ech-Cherif El Kettani, "Analysis of Identity Management Systems Using Blockchain Technology," 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, 2019, pp. 1-7, doi: 10.1109/COMMNET.2019.8742375.

[14] Faber, Benedict, et al. "BPDIMS: A blockchain-based personal data and identity management system." The 52nd Hawaii International Conference on System Sciences. HISS 2019: HISS 2019. Hawaii International Conference on System Sciences (HICSS), 2019.

[15] Alsayed Kassem, Jamila, et al. "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network." Applied Sciences 9.15 (2019): 2953.

[16] K. Mudliar, H. Parekh and P. Bhavathankar, "A comprehensive integration of national identity with blockchain technology," 2018 International Conference on Communication information and Computing Technology(ICCICT), Mumbai, India, 2018, pp. 1-6, doi: 10.1109/ICCICT.2018.8325891.

[17] Lim, Shu Yun, et al. "Blockchain technology the identity management and authentication service disruptor: a survey." International Journal on Advanced Science, Engineering and Information Technology 8.4-2 (2018): 1735-1745.

[18] Z. Chen and Y. Zhu, "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," 2017 IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, HI, USA, 2017, pp. 93-99, doi: 10.1109/AIMS.2017.31.

[19] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan and S. Wang, "An Identity Management System Based on Blockchain," 2017 15th Annual Conference on Privacy, Security and Trust (PST), Calgary, AB, Canada, 2017, pp. 44-4409, doi: 10.1109/PST.2017.00016.

[20] Do, Hoang Giang, and Wee Keong Ng. "Blockchain-based system for secure data storage with private keyword search." 2017 IEEE World Congress on Services (SERVICES). IEEE, 2017.

[21] Zyskind, Guy, and Oz Nathan. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE security and privacy workshops. IEEE, 2015.

[22] G. Xuan et al., "Identity Verification System Using Data Hiding and Fingerprint Recognition," 2005 IEEE 7th Workshop on Multimedia Signal Processing, Shanghai, China, 2005, pp. 1-4, dui: 10.1109/MMSP.2005.248583.