Volume 1 No 2, 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index
ISSN: 3049-2963

Blockchain for Secure Identity Management: A Review on Decentralized Authentication Systems

Dr. Nilesh Jain,
Associate Professor,
Department of Computer Science and Applications,
Mandsaur University, Mandsaur(M.P.)
nileshjainmca@gmail.com

***Abstract*—The rise of blockchain technology has revolutionized identity management by introducing decentralized, secure, and user-centric systems. The capacity of blockchain-based identity management solutions to circumvent the drawbacks of conventional centralized approaches is the primary emphasis of this analysis. Here, we take a look at several important ideas like decentralized trustworthy identity (DTI) and self-sovereign identity (SSI), and we see how they improve privacy and security while giving users more power over their own data. The paper also analyzes the role of cryptographic protocols, verifiable credentials, and decentralized identifiers (DIDs) in strengthening authentication processes. Despite its promise, blockchain-based identity management faces challenges, including scalability, privacy concerns, regulatory compliance, and system complexity. The purpose of this review is to offer a thorough overview of the present state of decentralized identity management by discussing the many approaches, problems, and potential avenues for further study in this area.**

Keywords*—Blockchain, Identity Management, Decentralized Authentication, Self-Sovereign Identity (SSI), Decentralized Trusted Identity (DTI), Verifiable Credentials, Decentralized Identifiers (DIDs), Privacy, Security, Scalability.

I. INTRODUCTION

There have been efforts to incorporate blockchain into the next generation of identity management solutions, capitalizing on blockchain's success. A vast number of dispersed nodes constitute a typical blockchain-based identity management system. Distributed computing, dependable access, and storage are all possible with these nodes. With this setup, the user's device or node can store sensitive personal data instead of servers, as is the case with traditional identity management solutions, and this is made possible by the new blockchain-based paradigm [1].

Establishing trust, enabling relationships, and facilitating access to resources in the digital domain are all built around identification. A person's digital identity can consist of several different things, including but not limited to: personal identifiers (email addresses, usernames, etc.), biometric data (fingerprints, face recognition, etc.), and cryptographic credentials (digital certificates, security tokens, etc.). Individuals' access to digital services, apps, and data is authorized by these IDs and traits, which also validate their identity. Digital identities go through a number of administrative tasks during their lifetime, including registration, authentication, authorization, and de-provisioning. This is all part of identity management [2].

Authentication serves as a fundamental cornerstone of online systems, functioning as the mechanism that establishes authorization for individuals or entities. Authentication plays a pivotal role in enabling users to protect their data and assert their identity. Authentication plays a pivotal role as a security measure, ensuring the protection of users in a landscape where all elements are distributed and stored. In particular, there is an urgent need for research into authentication technologies that have traditionally relied on centralized servers of authorities[3].

II. FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Every time a transaction is recorded and added to the blockchain's permanent database, it is called a block. Like a linked list, the blocks in a blockchain are connected in a sequential fashion. Hash values from prior blocks are included in each new block.

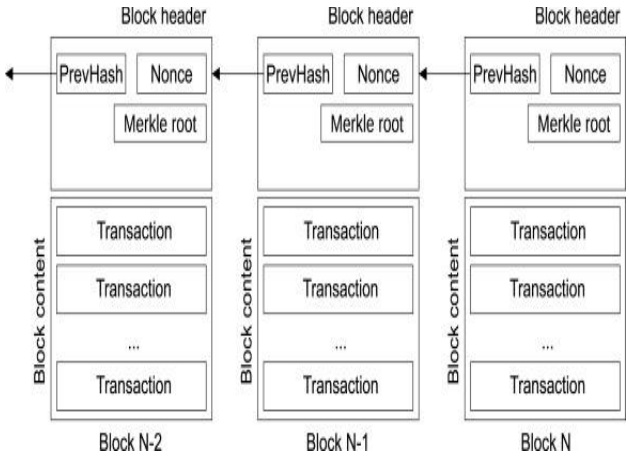

Fig. 1. Blockchain Architecture

A. *Key Elements Of Blockchain*

Here, we break out the fundamentals of blockchain design.

1) *Transaction*

A process that modifies the status of the blockchain ledger. Two alternative implementations of the transaction are the transfer of monetary value or the execution of a smart contract.

2) *Block*

There are two parts to this: the block header and the block data. A collection of valid transactions makes up the data, while the block's metadata including the timestamp, version, Merkle tree root hash, and hash of the previous block is contained in the header.

3) Merkle Tree Root Hash

Using a hashing technique, each transaction in the block is hashed separately. In order to get a single hash value, the hash values are first concatenated in pairs and then hashed again. The Merkle tree root hash value is the name given to this number.

4) Block Hash

A block's hash value is its unique identifier, and the block header is hashed twice to create it.

5) Previous Block Hash

A block's hash value is a representation of its predecessor in the chain. A block's parent is the block immediately preceding it. Each block incorporates the hash value of the previous block into its header to guarantee the immutability of the blockchain ledger.

6) Timestamp

This value represents the time at which the block was initially formed[4].

B. Types Of Blockchain

The specifics of the various blockchain types are given in this section. The following are the three categories of blockchains:

1) Public Blockchain

Public blockchains are among the most significant kinds of blockchains since they are both open and decentralized. Another interesting aspect of this Blockchain implementation is that computer networks are basically accessible to anyone interested in conducting transactions. Here, we're using two distinct Proof-of-work and Proof-of-stake models, and the validated person is effectively the one who gets the transaction incentives. Furthermore, there are no restrictions on the Public Blockchain, which is a decentralized ledger system. Anyone can access the data or a part of the Blockchain without needing permission. Any user with system access can be granted permission to access the data or a subset of the Blockchain[5].

2) Private Blockchain

Within this particular sort of Blockchain, the ability to view and submit transactions is restricted to either a single organization or all subsidiary organizations that belong to the same group. A third party is in charge of managing this system. Users are required to have the manager's authorization in order to engage in the activity. The only people who can view the transactions using this system are its members[6].

3) Hybrid Blockchain

Both public and private blockchains are incorporated into this system. Rather than a single body being in charge of administering the system, all of the members are in charge of maintaining the system and deciding who can take part in the blockchain [1], [7]. In addition to this, they decide which transactions are public and which are private[8].

III. BLOCKCHAIN-BASED IDENTITY MANAGEMENT SYSTEMS

The procedures and regulations that control the handling of an identity's attributes throughout its lifetime are collectively known as Identity Management (IdM). A single entity controls the majority of IdM schemes today [9]. Governments give national ID cards as an example of how the created identities can be federated outside a single organization. With federated identity systems, users can use the same identity information to access different security domains. Distributed ledger (DL) technology based on blockchain data structures has recently arisen as a new standard for digital IDMS. Its stated goals include user control, privacy, transparency, and decentralization. Self-sovereign identity (SSI) and decentralized trusted identity (DTI) are the two main types of DL-based IDMS[10].

A. Self-Sovereign Identity (SSI)

Persons in the digital world are seen more as users of online systems than as actual persons, according to the client-server model. This view holds that users need authentication, authorization, and identification in order to access and complete tasks on the internet. Because it is based on the premise that servers (companies, online enterprises) are more essential than clients (individuals), this digital model takes administrative precedence and dictates the rights of clients. Two crucial functions—VC and DID—are present at the heart of the SSI ecosystem [11].

1) Verifiable Credentials (VC)

A working group of the World Wide Web Consortium (W3C) standardized a specification called verifiable credentials (VCs)[12]. It is a digital substitute for traditional, paper-based identification documents like passports, national ID cards, and driver's licenses that is secure, machine-readable, and impossible to counterfeit. There are three identity holders: the provider and the verifier. Their interactions are based on a trust framework.

B. The Decentralized Identifiers (DIDs)

A novel form of globally unique identifier, the Decentralized Identifiers (DIDs) are defined in this specification. Their intended use is to facilitate the generation of unique identifiers by individuals and entities using reliable mechanisms. A decentralized identifier (DID) assigns a unique, permanent, cryptographically verifiable identifier to an individual, an organization, or an object on a worldwide scale. There is no need for a governing body when using a DID because the identity owner has complete power[13].

C. The Conceptual Difference Between SSI and DTI

There is little in the way of outward distinction between the two plans, but their core ideas set them apart.

- A centralized service can manage DTI by checking users' identities with a variety of government-issued credentials, including passports, national ID cards, driver's licenses, social security numbers, and more. Validated identity attestations are stored on a DL once verification is complete so that third parties can conduct additional verifications [14][15]. In fact, SSI eliminates the need for users to depend on preexisting third-party attestations by empowering them to fully own and control their own identities [16].
- Credentials obtained from various IdPs can then be used to acquire identity-related data. A user's identity is not linked to any central registry or IdP when using DTI[17].
- Permissionless or permissioned blockchains can be used to construct IDMS solutions based on SSI and

DTI. A solution's IMDS features are strongly dependent on the blockchain technology used to build it[18].

IV. Security And Privacy Considerations

A. Blockchain-Based Authentication Protocols

- When it comes to cryptographic protocols, authentication is key because it provides the base level of protection for information. Authentication protocols are standardized protocols that ensure the integrity, timeliness, and authenticity of messages during communication [19].
- Extensive research and study have been conducted on the topic of blockchain-based authentication systems due to their increasing focus in recent years [20].
- Safe authentication procedures frequently make use of cryptographic methods, including digital signatures, digital certificates, anonymous authentication, and group authentication [21].

B. Password Identity Authentication

- Among the many types of identity identification, the most basic is static password authentication, where users verify their identities by inputting pre-set static passwords. However, static password identity authentication has certain security vulnerabilities. For instance, passwords might be maliciously intercepted during transmission or be susceptible to being compromised.
- In contrast, dynamic password identity authentication is another form of password-based identity authentication. It relies on one-time passwords for identity verification, requiring users to utilize dynamically changing passwords generated by applications for each authentication attempt. Dynamic password identity authentication is more secure than static password identity authentication[22].

V. Challenges And Application

A. Challenges

In this section, we provide the details of what kind of challenges we face in securing identity management using blockchain.

1) Scalability

On large-scale blockchain applications, blockchain networks are capable of handling a large number of transactions. Scalable blockchain systems rely on data processing services since they are necessary for high-transaction execution [23]. The cloud's scalability makes it an attractive option for providing on-demand computing resources for blockchain-related tasks. Therefore, merging blockchain technology with cloud computing may lead to an integrated system that is extremely scalable [24][25].

2) Privacy

Another significant obstacle in the IdM System is privacy. For an effective IdM system, it is a must-have. In an IdM system, both the customer and the service provider are required to provide certain personally identifiable information. If users' privacy is compromised, service providers may be able to inappropriately use their personal information. Assuming security is intact, users should have greater say over their unique identity attributes to better protect their privacy[26].

3) Complexity Of Blockchain

Blockchain technology underscores its complexity. Although blockchain has many advantages, its complexity may prevent it from being widely used. The key to a smooth rollout of the technology in the banking industry is getting everyone involved on the same page.

4) Regulatory And Compliance Concerns

Laws and regulations are always changing to accommodate new forms of digital identification verification. Given the quick speed of technological changes, it can be challenging for banks to keep up with local and international standards regarding digital identity verification processes. Citations [27].

5) Performance

From the perspectives of energy and resources, throughput and latency, and capacity, we examine blockchain performance concerns. The most significant challenges for blockchain implementations pertain to energy, resources, throughput, and latency. Environmental sustainability would be advanced when blockchains were built with an affordable solution that may decrease mining energy consumption[24] In order to improve mining efficiency and prevent congestion, capacity management is crucial[27].

B. Application

In this section, we provide the details of the application of blockchain to secure identity management.

1) Authentication, Identity, And Access

Authentication, identity, and access each present their own unique set of challenges. Authentication is a prerequisite to gaining access to data and is a necessary step in the identification process. Due to privacy considerations specific to legal affairs, the complexities of authentication, identification, and access in law enforcement make these difficulties much more difficult to resolve. Digital governments that rely on transactions must have identification as one of their key components [28].

2) Healthcare Record Sharing

The exchange of medical records is at the heart of an early blockchain-based healthcare system. Because it involves the patient's private information, which is considered sensitive data, this is challenging. Blockchain technology's potential to gradually enhance people's quality of life makes it socially significant in the healthcare sector. Computing can alleviate some of the issues in this domain by applying the same reasoning. By facilitating more trustworthy data sharing, finding uses in other domains, and managing logs, informatics, for instance, aids in the automation of health records[29].

3) The Management Of Digital Identity

There are two key players in a digital identification model: the identity owner and the authorities. Both parties have certain rights and duties. To begin, control over one's own personal information ought to rest with the identity owner. Therefore, it is incumbent upon them to take precautions to prevent the loss or theft of the data It is the obligation of the identity owner to reveal their personal information whenever and with whoever they choose. The second point is that authenticating users is the job of the trusted authority. In

addition to managing the records, they also provide authentication proof and keep it in a database[30].

VI. Literature Review

The following section provides the literature review for A Review of AI-Driven Cloud-Native Distributed Systems: Architectures, Challenges, and Future Directions.

Yang et al. (2022) A deep forgery data identification and traceability framework based on blockchain is proposed in this study. To begin, we offer a blockchain-based approach to trustworthy data identification that creates a digital watermark inside the data and uses it to identify it. Second, implement a system for the forensic evaluation of electronic data that uses blockchain technology to check data for authenticity and similarity. The final step in achieving deep forgery data tracing and dissemination supervision is the development of a digital identification-based method[31].

Wang et al. (2023) Data storage management systems are the backbone of these systems, and this article primarily focusses on how blockchain technology is being applied to these systems. It also provides a brief analysis of the logic behind blockchain technology and how it is being applied to these systems. A blockchain-based approach to encrypted trusted data storage is suggested for asset metering. The data support for the trusted storage encryption of metering assets' underlying networks can be carried out by blockchain technology[32].

Zhu (2021) This study looks at how blockchain technology can be used in transactions involving digital financial assets, looks at the problems that blockchain technology is now facing in different industries that deal with digital financial asset transactions, and then offers solutions to those problems. Through the use of smart contracts, blockchain can integrate all types of industrial assets into a digital financial framework, creating an efficient digital asset management system. It has the potential to build an economic network that combines asset management with digitalization of financial assets, as well as to automate the mapping and circulation of assets under the chain[33]

Tabbassum et al. (2024) This study aims to give useful information for enterprises, governments, and researchers interested in deploying safe and decentralized identity management systems in a quickly expanding digital environment by synthesizing ideas from diverse sources. The idea of using blockchain technology for safe, decentralized identity management is examined in this study. We seek to investigate the possible advantages, difficulties, and practical applications of blockchain-based identity management systems through a thorough review of the existing literature, case studies, and real-world implementations[34].

Srivastava, Agarwal and Chaurasia. (2023) This paper proposes an effective model that integrates self-sovereign identity, oracle technology, and blockchain. This model aims to provide solutions and lay the groundwork for overcoming the challenges and ensuring the construction of a secure and reliable digital identity management system. blockchain technology has garnered in the field of digital identity management and the development of blockchain-based systems, these systems have not fully resolved the aforementioned problems. To address these issues and establish a secure and trustworthy digital identity management system[35].

Jadon et al. (2023) It offer a brief overview of current identity management methods that utilize blockchain technology in this article. We review the current approaches, note any holes or promising openings, and then provide a solution based on the mutable blockchain idea. Two algorithms have been implemented: one for creating new identities on the blockchain and another for updating current ones. The suggested algorithm's key feature is its ability to securely store personal data in a local database while simultaneously storing the hashed address of that data in the blockchain[36]

Xie (2024) focuses on the implementation of a decentralized identity authentication system and designs an innovative algorithm based on blockchain technology, aiming to improve the security, privacy, and decentralization of the system. The algorithm proposed in this study implements encrypted storage and distributed authentication of identity data through a distributed ledger and smart contracts of blockchain, ensuring the privacy and data security of users. The hash function and zero-knowledge proof method are introduced, so that the user's identity information does not need to be transmitted in plain text during the verification process, further improving the security of the authentication process[37].

Rahat et al. (2022) examine the usage of Blockchain technology to safeguard digital identities, a credible concept that explains how and what kinds of attributes or parameters can be utilized to identify individuals. A great deal of identity fraud occurs because people's personal information is utilized for many applications that are usually decentralized and any organization can have access to this data. The plan is to use Blockchain technology to create a single, secure identity that can serve several purposes[38].

VII. Conclusion And Future Work

Blockchain technology presents a transformative approach to secure identity management, shifting from centralized models to decentralized systems that enhance privacy, security, and user control. Through self-sovereign identities (SSI) and decentralized trusted identities (DTI), users gain unprecedented authority over their digital identities, reducing reliance on third parties and mitigating risks associated with centralized data breaches. While blockchain offers transparency, immutability, and cryptographic security, challenges such as scalability, regulatory compliance, and user privacy remain significant hurdles that must be addressed to fully realize its potential in identity management.

Future research should focus on developing scalable and privacy-preserving blockchain solutions tailored for identity management systems. Concerns about privacy can be addressed while preserving transparency by incorporating cutting-edge cryptographic techniques like zero-knowledge proofs and investigating hybrid blockchain solutions. Additionally, creating standardized frameworks for regulatory compliance and interoperability across different blockchain platforms will be critical. Emphasis on user-centric designs and real-world pilot implementations can further validate the efficacy and adoption of decentralized identity management systems in various sectors, from finance to healthcare.

References

[1] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, “Blockchain-based identity management systems: A review,” *J. Netw. Comput. Appl.*, vol. 166, p. 102731,

Sep. 2020, doi: 10.1016/j.jnca.2020.102731.

[2] K. Jasper, A. S. Vignesh Raja, R. Neha, S. Suman Rajest, R. Regin, and B. Senapati, "Secure Identity: A Comprehensive Approach to Identity and Access Management," *FMDB Trans. Sustain. Comput. Syst.*, vol. 1, no. 4, pp. 171–189, 2023.

[3] J. Seo, "The Future of Digital Authentication: Blockchain-driven Decentralized Authentication in Web 3.0," *J. Web Eng.*, vol. 23, no. 5, pp. 611–636, Aug. 2024, doi: 10.13052/jwe1540-9589.2351.

[4] L. Ismail and H. Materwala, "A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions," *Symmetry (Basel).*, vol. 11, no. 10, p. 1198, Sep. 2019, doi: 10.3390/sym11101198.

[5] P. K. Paul, "Blockchain Technology and its Types—A Short Review," *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, Dec. 2021, doi: 10.30954/2322-0465.2.2021.7.

[6] M. K. Shrivas, "The Disruptive Blockchain: Types, Platforms and Applications," *TEXILA Int. J. Acad. Res.*, pp. 17–39, Apr. 2019, doi: 10.21522/TIJAR.2014.SE.19.01.Art003.

[7] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, New York, NY, USA: ACM, Jan. 2012, pp. 326–349. doi: 10.1145/2090236.2090263.

[8] D. A. Luong and J. H. Park, "Privacy-Preserving Identity Management System on Blockchain Using Zk-SNARK," *IEEE Access*, vol. 11, pp. 1840–1853, 2023, doi: 10.1109/ACCESS.2022.3233828.

[9] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in *Proceedings of the 2016 USENIX Annual Technical Conference, USENIX ATC 2016*, 2016.

[10] P. Dunphy and F. A. P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 20–29, Jul. 2018, doi: 10.1109/MSP.2018.3111247.

[11] F. Schardong and R. Custódio, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," *Sensors*, vol. 22, no. 15, p. 5641, Jul. 2022, doi: 10.3390/s22155641.

[12] Z. Gao *et al.*, "Blockchain-based Identity Management with Mobile Device," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, New York, NY, USA: ACM, Jun. 2018, pp. 66–70. doi: 10.1145/3211933.3211945.

[13] A. Thorve, M. Shirole, P. Jain, C. Santhumayor, and S. Sarode, "Decentralized Identity Management Using Blockchain," in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, IEEE, Dec. 2022, pp. 1985–1991. doi: 10.1109/ICAC3N56670.2022.10074477.

[14] G. Deep, R. Mohana, A. Nayyar, P. Sanjeevikumar, and E. Hossain, "Authentication Protocol for Cloud Databases Using Blockchain Mechanism," *Sensors*, vol. 19, no. 20, p. 4444, Oct. 2019, doi: 10.3390/s19204444.

[15] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informatics J.*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[16] 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," *IEEE Access*, vol. 10, pp. 113436–113481, 2022, doi: 10.1109/ACCESS.2022.3216643.

[17] S. Cucko and M. Turkanovic, "Decentralized and Self-Sovereign Identity: Systematic Mapping Study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021, doi: 10.1109/ACCESS.2021.3117588.

[18] A. E. Panait, R. F. Olimid, and A. Stefanescu, "Identity management on blockchain – Privacy and security aspects," *Proc. Rom. Acad. Ser. A - Math. Phys. Tech. Sci. Inf. Sci.*, 2020.

[19] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, "A Secured Privacy-Preserving Multi-Level Blockchain Framework for Cluster Based VANET," *Sustainability*, vol. 13, no. 1, p. 400, Jan. 2021, doi: 10.3390/su13010400.

[20] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Networks*, vol. 6, no. 2, pp. 177–186, May 2020, doi: 10.1016/j.dcan.2019.04.003.

[21] X. Luo, X. Chen, X. Chen, and Q. Cheng, "A survey on the application of blockchain in cryptographic protocols," *Cybersecurity*, vol. 7, no. 1, p. 79, Dec. 2024, doi: 10.1186/s42400-024-00324-7.

[22] J. Li, "A review of identity authentication based on blockchain technology," *Appl. Comput. Eng.*, 2024, doi: 10.54254/2755-2721/30/20230094.

[23] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment," *J. Med. Syst.*, vol. 42, no. 8, p. 156, Aug. 2018, doi: 10.1007/s10916-018-1007-5.

[24] C. V. N. U. B. Murthy and M. L. Shri, "A Survey on Integrating Cloud Computing with Blockchain," in *International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE 2020*, 2020. doi: 10.1109/ic-ETITE47903.2020.470.

[25] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing," *Futur. Internet*, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.

[26] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5782–5796, Sep. 2022, doi: 10.1016/j.jksuci.2021.03.005.

[27] T.-V. Le Tuan-Vinh Le and C.-L. H. Tuan-Vinh Le, "A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges," 網際網路技術學刊, vol. 22, no. 4, pp. 789–801, Jul. 2021, doi: 10.53106/160792642021072204007.

[28] L. J. Camp, "Digital identity," *IEEE Technol. Soc. Mag.*, vol. 23, no. 3, pp. 34–41, 2004, doi: 10.1109/MTAS.2004.1337889.

[29] P. K. Ghosh, A. Chakraborty, M. Hasan, K. Rashid, and A. H. Siddique, "Blockchain Application in Healthcare Systems: A Review," *Systems*, vol. 11, no. 1, p. 38, Jan. 2023, doi: 10.3390/systems11010038.

[30] A.-C. Careja and N. Tapus, "Digital Identity Using Blockchain Technology," *Procedia Comput. Sci.*, vol. 221, pp. 1074–1082, 2023, doi: 10.1016/j.procs.2023.08.090.

[31] K. Yang, D. Li, Q. Guo, H. Wang, D. Bai, and X. Pan, "Research on Deep Forgery Data Identification and Traceability Technology Based on Blockchain," in *2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA)*, IEEE, Oct. 2022, pp. 230–234. doi: 10.1109/ICDSCA56264.2022.9988274.

[32] X. Wang *et al.*, "Application of data storage management system in blockchain-based technology," in *2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)*, IEEE, Feb. 2023, pp. 1437–1440. doi: 10.1109/EEBDA56825.2023.10090564.

[33] Y. Zhu, "Research on Digital Finance Based on Blockchain Technology," in *2021 International Conference on Computer, Blockchain and Financial Development (CBFD)*, 2021, pp. 410–414. doi: 10.1109/CBFD52659.2021.00089.

[34] A. Tabbassum, P. Chintale, C. Akiri, and N. Bhasin, "Leveraging Block chain for Secure and Decentralized Identity Management," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 2024, pp. 1–6. doi: 10.1109/ICBDS61829.2024.10837296.

[35] S. Srivastava, D. Agarwal, and B. Chaurasia, "Secure Decentralized Identity Management using Blockchain," in *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2023, pp. 1355–1360. doi: 10.1109/TrustCom60117.2023.00185.

[36] S. Jadon, D. A. Bhat, S. R, Y. TB, and P. HB, "Mutable Blockchain for Identity Management," in *2023 4th International Conference on Innovative Trends in Information Technology (ICITIIT)*, 2023, pp. 1–4. doi: 10.1109/ICITIIT57246.2023.10068675.

[37] Y. Xie, "Research on Blockchain Implementation Algorithm for Decentralized Identity Authentication System," in *2024 IEEE 4th*

International Conference on Data Science and Computer Application (ICDSCA), 2024, pp. 572–577. doi: 10.1109/ICDSCA63855.2024.10859590.

[38] A. H. Rahat *et al.*, "Blockchain Based Secured Multipurpose Identity (SMID) Management System for Smart Cities," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, pp. 737–744. doi: 10.1109/CCWC54503.2022.9720808..

