IJDI-ERET

INTERNATIONAL JOURNAL OF DARSHAN INSTITUTE ON ENGINEERING RESEARCH AND EMERGING TECHNOLOGIES
Vol. 12, No. 1, 2023
www.ijdieret.in

(Review Article)

Identity Management using Blockchain - A Review

Abhishek Bamnote[1*], Rachana Patil[2]

[1*,2]*Department of Computer Engineering, PCCOE - Pimpri Chinchwad College Of Engineering, Pune, Maharashtra, INDIA*

Abstract

In recent years, the management of identity, identity theft, and fake identities has become a more significant issue. In our society, maintaining trust and security is always a concern. With time and digitalization, the human race has found many ways to protect individual identities. A good example can be a passport worldwide or an Aadhar card in India. Still, we can always have news about fake documents, even while documents are being digitized. To prevent identity theft and fake identity issues, we can use blockchain technology to link multiple documents together. This would involve the history of that person due to the linking of every past document. The documents are to be verified before being uploaded by authorities and signed by the issuing institution. The authority to access the information should be given only to the holder. Another aspect of how much information should be revealed must be a concern. In this paper, we would like to review some possible solutions to all these problems.

Keywords: Blockchain, EBSI, Identity Management, Smart Contracts, Self-Sovereign Identity (SSI), Zero-Knowledge Proof.

1. Introduction

There has been a surge in identity and documentation-based crimes; there is a need for a system that can be useful in reducing crime and helping manage documents and identity in a much more effective way. The sharing of documents among institutions and people needs to be managed so that information is not leaked [1]. Document sharing should be limited to the information needed for verification. For this, we can use the latest technology, like blockchain. A self-sovereign identity approach should be used to provide and handle information.

Blockchain is a technology in which a distributed database is used to record all the transactions with the help of a network that is based on the concept of the peer-to-peer network. It was successful in solving the trust issues related to the centralized party [2, 3]. Bitcoin was one of the first applications of blockchain, which brought blockchain as a technology into the limelight. After the introduction of bitcoin, Ethereum (ETH) extended the use of blockchain, introducing smart contracts. Smart contracts are agreements that are coded on top of the blockchain to ensure trust between two parties without the involvement of a third party. This helped blockchain take paper-based contracts all the way to digital contracts due to its immutability.

[*]*Corresponding Author: e-mail: abhi2bamnote@gmail.com, Tel-+91-7083386048, +91-9503956332*
ISSN 2320-7590 (Print) 2583-3863 (Online)
© 2023 Darshan Institute of Engg. & Tech., All rights reserved

Self-Sovereign Identity (SSI) is a concept describing the digital identity of any individual who has complete control over the information to be provided to any institution, website, or service. As per the paper [4], the solution for digital identity has been around since 1976, when the Diffie-Hellman Key Exchange algorithm was introduced.

Identity management (IdM), also known as identity and access management (IAM), guarantees that only authorized individuals have access to the information technology resources they require to execute their jobs. It encompasses policies and technology that encompass an enterprise-wide process to properly identify, authenticate, and authorize individuals [5], groups of individuals, or software applications through attributes such as user access privileges and restrictions depending on their identities.

There are a significant number of distributed nodes in a typical blockchain-based identity management system. These nodes may be used to provide distributed storage, dependable access, and computation capabilities. In such a system, the user operates as a network node, permitting the storage of sensitive user data to migrate from servers (in conventional identity management solutions) to user devices/network nodes (in the new blockchain-based paradigm). This supports self-sovereign identification (SSI), as users will be able to reclaim control over their own identity. As a result, several dangers inherent to conventional identity management solutions are mitigated.

The major parts of identity management are Identity establishment, identity access management, and attribute management. The establishment process deals with uploading

data about a particular person to create a digital identity. Identity access management deals with the authorization and authentication of data being uploaded [6]. Then attribute management deals with the sharing of relevant data when needed. This concept is strongly linked to the idea of Zero Knowledge Proof.

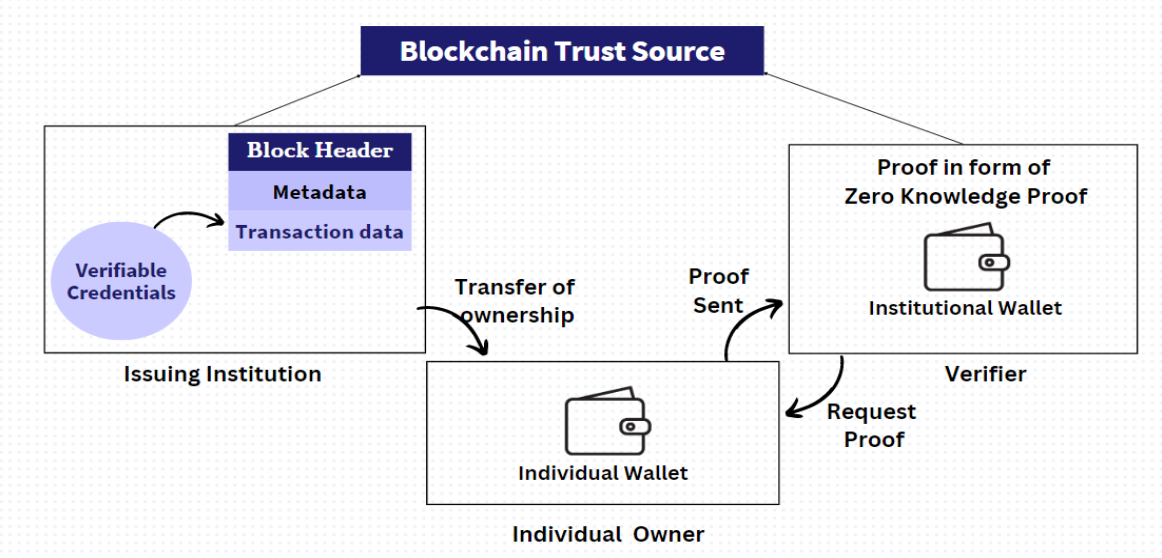

Figure 1. Blockchain based identity management

2. Literature Survey

Blockchain and its real life applications include bitcoin, ethereum, smart contracts, and decentralization. Smart contracts' decentralization, auto-enforcing capability, and verifiability features allow their encoded business rules to be carried out in a peer-to-peer network where each node is "equal" and has no special power without the assistance of a centralized server or trusted authority. Smart contracts facilitate, carry out, and enforce agreements between untrustworthy parties without the assistance of a trustworthy third party. On top of the blockchain, smart contracts are programmable scripts that may be executed. Smart contracts are executable scripts that operate on top of the blockchain. Smart contracts may be used to automate the transfer of different forms of ownership of assets, property, and value, which makes working procedures more transparent and less mediated. [1] The concerns with the blockchain, including scalability, immutability, consensus mechanisms [7], and dependency on "off-chain" resources, are also covered in this study.

Self-Sovereign Identity, Zero-Knowledge Proof, Generic Provable Claims, and Chains of Claims are a few of the building blocks of a blockchain based identity management system. Self-Sovereign Identity (SSI) is a concept describing the digital identity of any individual who has complete control over the information to be provided to any institution, website, or service. The discussed implementations are IPv8, Identity Chain, Group A, and Group B. [9] Zero knowledge proof is described as a method to verify information without oversharing data to prevent data leaks.

The structure of a block and a decentralized identifier are the basic blocks of an identity management system. The use of claims in the implementation of Identity management systems is to identify certain properties, their relation to the subject, and their value. The verifiable credential is linked into two parts: the credential graph and the proof graph. The credential graph consists of attributes like issue date, type, information, and issuer. The proof graph consists of attributes like signature, creator, signature date, public key, and signature type. These credentials are used in the blocks as they are structured and chained together. [10] This complete, verifiable credential has at least one claim, which is in the form of the signature of the issuer.

The (very utopian) notion of self-sovereign identity holds that individuals and organizations should be more in charge of their physical and digital identities. Everybody, including every organization, has a special set of identifying data, such as a business license or a university degree. This notion seems to provide a solution to the issues of data control and internet privacy. To put it another way, because they are no longer obligated to disclose their identifying information to numerous databases, a person's or organization's risk of having their identity and identifying information stolen by criminals is significantly reduced. Theoretically, the first step would be to digitize every analogue document, including birth certificates, business licenses, and university degrees, and save it as a single digital record in the possession of the individuals or organizations that issued it. [12] Every piece of identifying information could theoretically be stored in a single, secure "digital wallet." As a shared database that records transactions, blockchain may be used to implement SSI in the real world by

utilizing its concepts of immutability and security.

The Identity Access Control process for this particular topic of blockchain based identity management systems. The project was under the author's close observation from the beginning to the end [13]. No input was offered until the answer was delivered in order to prevent affecting the project. The deliverables were critically examined using the concepts and ideas from the literature review. The findings were reviewed with all pertinent parties and contrasted with the project manager's report. The author's conclusions are listed below, and they have been verified by the pertinent parties. To eliminate prejudice, an effort has been made to generalize the project's qualities and outcomes and match them with literary themes. [14]

A zero-knowledge protocol of Interval membership utilizing the Pedersen commitment scheme is used to protect the privacy of specific user identity attributes. This paper describes how user attributes can be kept anonymous over the block chain in a selective manner.[16] A novel system for secure mutual authentication, applicable to smart homes and other applications.[17] In particular, the proposed method combines blockchain, group signature, and message authentication code to provide dependable auditing of user access history, anonymously authenticate group members, and efficiently authenticate the home gateway, respectively.

3. Workflow and Flow Diagrams

The flow for the following model based on reviewed papers can be defined in major four parts as shown in Figure (2). The parts in which we can define are:

- Blockchain blocks for the following model.[2]
- Verifiable credentials and attributes in them.[3]
- Transfer of information between institutions and owners.[4]
- Identity Access Control.[6]

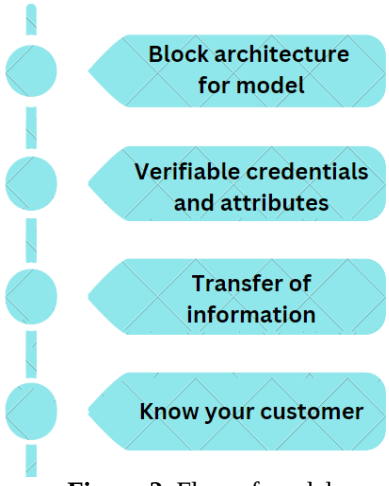

Figure 2. Flow of model

3.1 Blockchain blocks for the following model: Figure 3 depicts a chain entry, or block, in the passive model. These passive model blockchain blocks can be formatted in one of two ways: a claim of origin (Figure 3a) or a simple attestation (Figure 3b). As implied by its name, the claim origin is where the first claim metadata is stored on a blockchain. This claim might possibly be uploaded to the blockchain without any attestation from an attesting party.

However, as no claim is valid without supporting evidence, the block is only added to the chain as an optimisation after the first proof is gathered. After the initial attesting party signs the claim, the double-signed block is added to the chain. Further attestations for the same claim can then be obtained by the user. However, it is no longer necessary to store the entire claim with further attestations for the same claim. As shown in Figure 3b, additional attestations can simply sign for the block hash of the block containing the claim to avoid data duplication. [15]

3.2 Verifiable credentials and attributes in them: An identity owner may choose to selectively share specific identity data in order to safeguard their privacy. This enables identification while upholding the maxim of just exposing what is absolutely necessary in any particular circumstance.

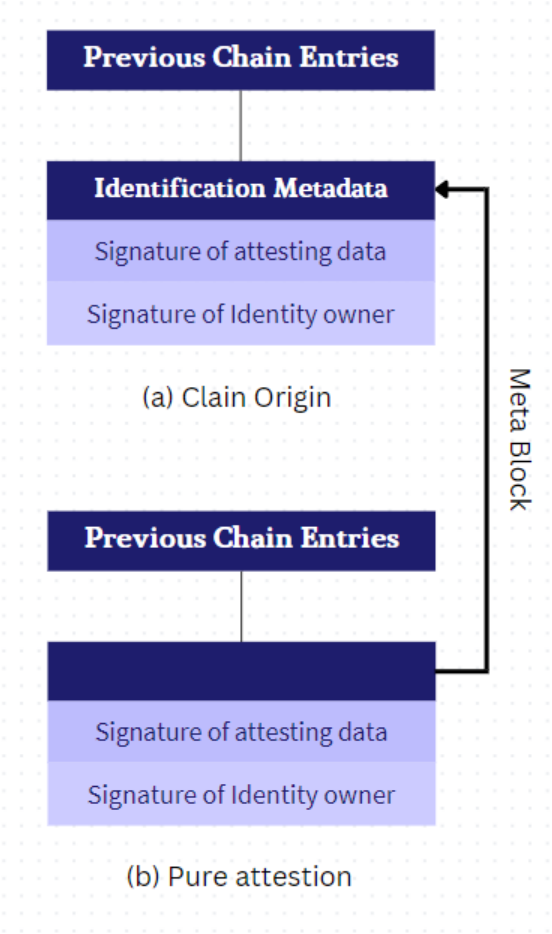

Figure 3. Structure of the blocks. [23]

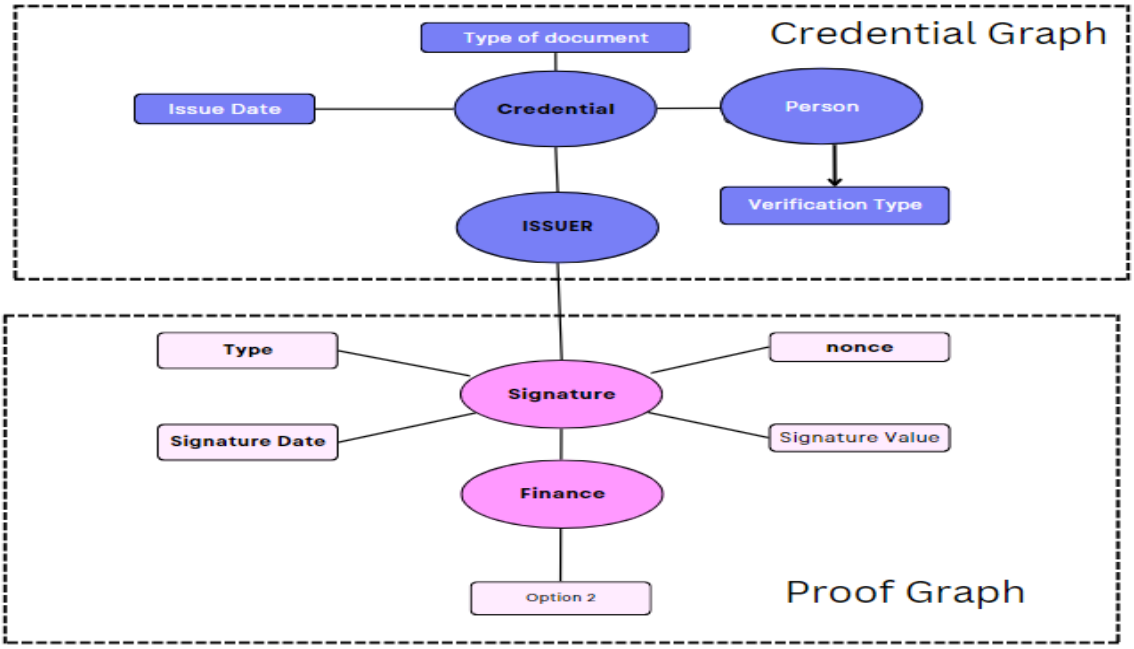

Figure 4. Relations and structure of attributes [23]

A Verifiable Presentation is the term used to describe the representation of such a subset of identification data.

The structure of Verifiable credential as shown in Figure 4 can be defined as:

- At first, the values of attributes in the credential graph are taken.
- Then values are inserted in the credential graph.
- A proof graph is then created.
- Then, the issuer authority signs the proof graph.
- Both credential graph and proof graph are chained together.
- This complete, verifiable credential is then used to blocks.

3.3 Verifiable credentials and attributes in them: Consent and privacy are guaranteed by design when ESSIF principles and methods are used. The digital credential's owner (holder) will always initiate communications with third-party services, receive data verifiable attestations, and distribute data verifiable presentations.

The communication between all the actors in Figure 5 is as:

- We have three actors in this scenario, which are the issuing institute, the owner, and the verifying institute.
- The communication starts with the issuing institute issuing the document for an individual.
- The document is then uploaded to the blockchain based trust source, and ownership is transferred to the owner of the document.
- When any other institute wants to verify a document, the owner needs to grant permission to view the information.
- Once permission is granted, information can be verified by the institute via the blockchain-based trust source.

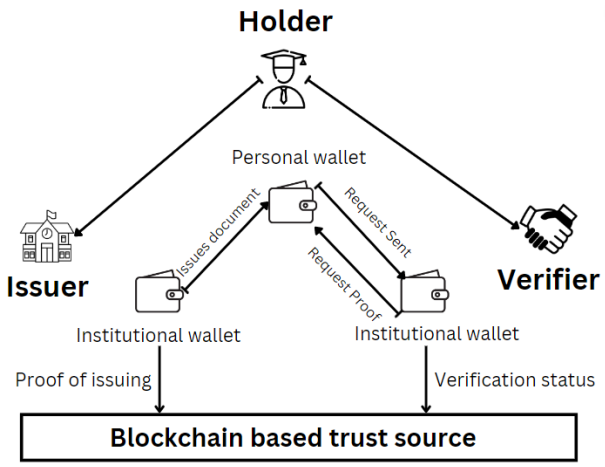

Figure 5. Ownership transfer diagram.

3.4 Identity access control: Only when at least one set of qualities is made available by an organization other than the one the client is trying to join will this procedure be effective.

- This process will only be successful if an organization other than the one the client is attempting to join makes at least one set of qualities available.
- The customer must input the server URL for the new company they wish to onboard.

- The organization's server receives the current identification.
- The server verifies the clients' identities and delivers a list of products.
- The consumer selects a product and sends their selection to the server.
- The server gives the client the initial on-boarding form.
- The option to share a form that has previously been verified is provided if there are forms that share attributes with another organization. Otherwise, the client completes the form, includes any necessary attachments, and submits it to the server.
- The server signs the form on the blockchain and, if necessary, transmits the next form.
- The server sends the client a verification following each seal.
- The server notifies the customer after CDD onboarding and all associated operations are complete. [6]

4. Analysis of Literature Review

The analysis of the following literature review can be summarized in a comparison table (1).

5. Conclusion

In this paper, we have studied how we can manage a digital identity with the help of rapidly growing technology like blockchain. Blockchain, still in its early stages, has vast potential for future applications. We studied the concept of self-sovereign identity and its importance. With the help of chaining in blockchain, we explained the secureness of the model. Zero knowledge proof helps us share information without fear of data leaks. The model of EBSI was useful in terms of the sharing of documents within institutions and owners, while Identification Access Control was used to share information while being secure.

Table 1. Advantages and disadvantages of reviewed systems

Name	Advantages	Disadvantages
Self-Sovereign digital identity on the European blockchain services infrastructure[9]	• DID or Digital identifier is used so that any decentralized identifier system can use it. • Structure for verifiable credentials.	Does not explain the transfer of ownership.
Deployment of a blockchain-based self-sovereign identity[10]	• Achieving Self Sovereign Identity (SSI). • Legally validating signatures.	Does not explain the transfer of ownership.
Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education[11]	Explains the transfer of ownership of documents within institutes and individuals.	Unable to explain verification and structure of documents for the system.
Towards self-sovereign identity using blockchain technology[12]	• Proper implementation of a blockchain based identity management system is explained. • A zero knowledge proof based information sharing system is proposed.	Verification of documents is a major problem in this implementation
Anonymity: A secure identity management using smart contracts[16]	Commitment and zero-knowledge protocol, the discretionary anonymity of the user's assets on the blockchain.	It may cost much for large scale implementation.
HomeChain: A blockchain-based secure mutual authentication system for smart homes[17]	More effective in the capacity to dynamically add or remove nodes and edges, demonstrate the security of proposed TCUGA in the standard model, and evaluate its performance to demonstrate its feasibility versus BIMS.	Requestors may be used to deceive other users by acquiring multiple certificates for a single node.
DNS-IdM: A blockchain identity management system to secure personal data sharing in a network[18]	Circumvent the limitations and vulnerabilities of identity attributes, including persistence, request, and verification, as well as overhead and security.	It is necessary to identify the facilitators and obstacles for blockchain-based identity management services in developing compliance with digital standards.
Identity and access management with blockchain in electronic healthcare records[19]	On the basis of hyperledger fabric, a decentralized, efficient, and secure simulation was created.	Not very scalable.
Identity management in healthcare using blockchain technology[20]	Decentralised and more transparent.	Potential vulnerabilities may be exploited by adversaries to threaten the security of the Healthcare sector.

References

[1] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021, doi: 10.1007/s12083-021-01127-0.

[2] G. Pattewar, N. Mahamuni, H. Nikam, O. Loka, and R. Patil, "Management of IoT Devices Security Using Blockchain—A Review," in *Sentimental Analysis and Deep Learning*, S. Shakya, V. E. Balas, S. Kamolphiwong, and K.-L. Du, Eds., Singapore: Springer Singapore, 2022, pp. 735–743. doi: 10.1007/978-981-16-5157-1_57.

[3] S. Deore, R. Bachche, A. Bichave, and R. Patil, "EHR-Sec: A Blockchain Based Security System for Electronic Health," in *Soft Computing and Signal Processing*, V. S. Reddy, V. K. Prasad, J. Wang, and K. T. V. Reddy, Eds., Singapore: Springer Nature Singapore, 2022, pp. 295–303. doi: 10.1007/978-981-16-7088-6_26.

[4] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada: IEEE, Jul. 2018, pp. 1336–1342. doi: 10.1109/Cybermatics_2018.2018.00230.

[5] R. Patil and Y. H. Patil, "A Secure and Efficient Identity based Proxy Signcryption Scheme for Smart Grid Network," *Journal of Engineering Science and Technology Review*, vol. 15, no. 4, pp. 82–89, 2022, doi: 10.25103/jestr.154.12.

[6] R. Y. Patil, A. Karati, Y. Patil, and A. Bannore, "Reliable data sharing in medical cyber physical system using fog computing," in *Intelligent Edge Computing for Cyber Physical Applications*, Elsevier, 2023, pp. 67–83. doi: 10.1016/B978-0-323-99412-5.00007-1.

[7] M. Borse, P. Shendkar, Y. Undre, A. Mahadik, and R. Y. Patil, "A Review of Blockchain Consensus Algorithm," in *Expert Clouds and Applications*, I. J. Jacob, S. Kolandapalayam Shanmugam, and R. Bestak, Eds., Singapore: Springer Nature Singapore, 2022, pp. 415–426. doi: 10.1007/978-981-19-2500-9_31.

[8] Z. Wang *et al.*, "On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy," 2022, doi: 10.48550/ARXIV.2201.09035.

[9] P. Altmann and E. Rissanen, "Self-Sovereign Digital Identity on the European Blockchain Services Infrastructure," 2020, doi: 10.13140/RG.2.2.30892.49281.

[10] R. Seifert, "Digital identities – self-sovereignty and blockchain are the keys to success," *Network Security*, vol. 2020, no. 11, pp. 17–19, Nov. 2020, doi: 10.1016/S1353-4858(20)30131-8.

[11] A. Grech, I. Sood, and L. Ariño, "Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education," *Front. Blockchain*, vol. 4, p. 616779, Mar. 2021, doi: 10.3389/fbloc.2021.616779.

[12] D. S. Baars, "Towards self-sovereign identity using blockchain technology," Oct. 2016. http://essay.utwente.nl/71274/ (accessed May 31, 2023).

[13] N. M. Shekokar *et al.*, *Cyber Security Threats and Challenges Facing Human Life*, 1st ed. Boca Raton: Chapman and Hall/CRC, 2022. doi: 10.1201/9781003218555.

[14] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, p. 102731, Sep. 2020, doi: 10.1016/j.jnca.2020.102731.

[15] M. Kuperberg, "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[16] Y. Borse, A. Chawathe, D. Patole, and P. Ahirao, "Anonymity: A Secure Identity Management Using Smart Contracts," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3352370.

[17] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K.-K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 818–829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400.

[18] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: A Blockchain Identity Management System to Secure Personal Data Sharing in a Network," *Applied Sciences*, vol. 9, no. 15, p. 2953, Jul. 2019, doi: 10.3390/app9152953.

[19] T. Mikula and R. H. Jacobsen, "Identity and Access Management with Blockchain in Electronic Healthcare Records," in *2018 21st Euromicro Conference on Digital System Design (DSD)*, Prague: IEEE, Aug. 2018, pp. 699–706. doi: 10.1109/DSD.2018.00008.

[20] J. P. N. dos Santos, "Identity management in healthcare using blockchain technology," masterThesis, Universidade de Évora, 2018. Accessed: May 31, 2023. [Online]. Available: http://dspace.uevora.pt/rdpc/handle/10174/24008

[21] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, p. 102731, Sep. 2020, doi: 10.1016/j.jnca.2020.102731.

[22] 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*, vol.

34, no. 8, pp. 5782–5796, Sep. 2022, doi: 10.1016/j.jksuci.2021.03.005.

[23] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, Oct. 2021, doi: 10.1007/s12599-021-00722-y.

Biographical notes

Abhishek Bamnote is a third year computer engineering student at Pimpri Chinchwad College of Engineering, India. He is a web development and blockchain development enthusiast.

Rachana Y. Patil received PhD from University of Mumbai, India in 2020. She has published 40+ papers in international journals and conferences. Her primary area of research is Cryptography, Network Security, Cyber Security and Digital Forensics (specially Network forensics). She is a Member of IEEE, ACM and IETE.