All Sciences Proceedings

1st International Conference on Recent Academic Studies

May 2-4, 2023 : Konya, Turkey

ICRAS

All Sciences Proceedings
http://as-proceeding.com/

https://as-proceeding.com/index.php/icras

A Systematic Review of Blockchain-based Identity Management Solutions

Huda Seyam [*], Adib Habbal [2]

[1]Computer Engineering Department / Faculty of Engineering, Karabuk University, Türkiye

[*]huda.s.seyam@gmail.com, adibhabbal@karabuk.edu.tr

***Abstract* –** The involvement of digital identity in almost all online services contributes to the growing reliance on Identity Management Systems (IDMS) that establish, verify, and manage digital identities. However, digital identities are still kept in central repositories. Which are controlled by a single authority that may have many vulnerabilities due to low security, leading attackers to exploit these vulnerabilities and causing various security breaches such as identity theft or disclosure of sensitive information. Additionally, powerful entities who have access to these repositories, could gather and abuse users' information without their knowledge or consent. The concept of Self-sovereign Identity (SSI) allows users to exert ownership of their identity and gain insight into how their data is being used. The development of Blockchain technology has made a breakthrough in achieving SSI by giving individuals the ability to be the final arbiter of who can access and use their own identity. This paper overviews the traditional identity management (IdM) models and presents the next generation of distributed IDMS using Blockchain technology that targets user-centricity and eliminates the identity provider as a trusted third party. Furthermore, It gives an analysis of the recent Blockchain-based IdM solutions, discussing their architecture, components, and features. It also, reveals their weaknesses to identify the gaps between these solutions for future secure IDMS.

Keywords – Digital Identity, Identity Management, Self-sovereign Identity, Decentralization, Blockchain.

I. INTRODUCTION

The significant amount of time that people spend on the Internet keeps climbing too especially, with the spread of the COVID-19 pandemic. This leads to increase the usage of online services. As a result, most of the individuals today has a kind of online identity. Digital identity refers to the personal identity in cyberspace that define a person and distinguished him from another person [1]. The identity is established and maintained by that person. Whereby the complete personal identity is the combination of all his attributes. The user identity is the general name given to the profile information in the user's account such as username, email address, birthday, etc. [2].

Individuals' digital identities are stored in central repositories. This exposed us to many centralization risks, including Single Point Of Failure (SPOF), and controlled by third-party entities that have the entire control of our personal information [1]. The huge amount of personal data that we leave behind while using online services could be misused by platforms. This information may include addresses, telephone numbers, full names, etc. In 2016, the Cambridge Analytica scandal happened when Facebook breached the privacy of its users and leaked internal emails between the Cambridge Analytica firm and the British parliament [3]. Furthermore, identity owners need to repeat registering and authenticating their identity information across different platforms in order to access their service. As a result, digital identity information will be fragmented, overshared, and unable to flow between different platforms [4]. Thus, it requires a new approach for IDMS to address these issues and meets with users' privacy requirements.

Building on the success of Blockchain technology, researchers began to investigate the effectiveness of using Blockchain to overcome some of the issues experienced by most central repositories. Since Blockchain is a tamper-resistant database, ensures that the block data is trustworthy. Therefore, Blockchain helps to deliver a trust infrastructure in IDMS.

II. BACKGROUND

In this section, we introduce the preliminaries of digital identity, IdM and the evolution of IdM models, followed by an overview of Blockchain technologies.

Identity Management

Digital identity has been key for allowing individuals to interact with service providers. Where identity refers to the combination of identifiers and credentials of entities in an appropriate context such as entity username, email address, preferences, and other entity attributes [2]. IDMS broadly refers to the framework of policies and technologies designed to ensure that only authorized users have access to associated resources. Also, it facilitates managing and securing users' digital identities and provides relevant services such as authentication[5].

IDMS consists of three main entities[6]:

User: the subject or the owner of certain attributes or credentials and could use various services provided by service providers and identity providers.

Service Provider: Is an important entity of the management system, responsible for providing services to successfully authenticated users.

Identity Provider: The issuer of identity information for users. it is the core entity of the management system, responsible for providing users with identity services.

A. *Identity Management Models*

We will discuss the main IdM models and highlights their advantages and limitations. Also, presented the new Blockchain-based approach for IdM.

Independent Identity Model. Also known as isolated IdM. In this model users didn't have their own identities, they only had accounts on a different service provider. Every service provider has its own identity provider as shown in Fig. 1. The identity provider assigns a unique identifier for each user. identifiers such as username and password [1]. Although the structure is simple, it requires a high storage capacity for each service provider. Also, the user needs to repeat the registration process which drives him to reuse the same password for many service providers. This creates a security concern as a compromise at one service provider can result in account hijacking at a different service provider. Moreover, the user needs to manage all his fragmented accounts among different service providers.

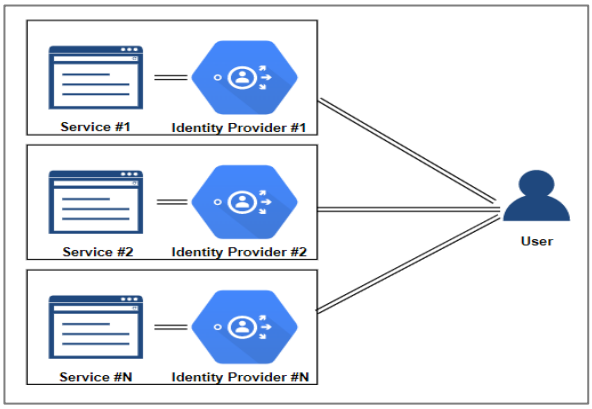

Fig. 1 Independent Identity Model

Centralized Identity Model. In this model, only one identity provider as a separate entity within a trusted domain is responsible for both identification and authentication. Thus, allowing any service provider belonging to the trusted domain to share users' identities. The users' credentials are verified by a central authority. In the identification process, the user needs to identify himself to the identity provider. The identity provider verifies the user's identity through an authentication process. After completion of authentication, the user receives a token from the identity provider, and he passes the token to the service provider. Then the service provider verifies the user credentials that are carried in the user's token by querying the identity provider. After successful validation, the user can use the requested service within a certain amount of time that is determined in his token [7]. Fig. 2 illustrates the process in the centralized identity model.

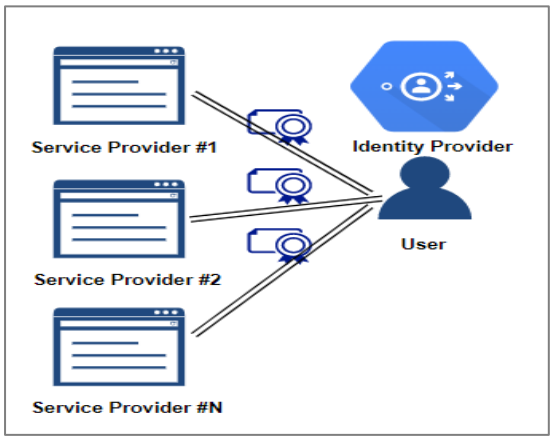

Fig. 2 Centralized Identity Model

Federated Identity Model. In this model, multiple service providers within a trusted domain called federation agreed to work together to confederate and share their users' identities information [8]. Thus, allowing any service provider belonging to the federation to identify users easily. We know this on the web as social login using Google or Facebook, etc. The high-level architecture of the federated identity model is presented in Fig. 3. This model allows users to sign up once and carry their identity information to other service providers by using the same set of credentials. Thus, reduces the number of passwords needed to access all services down to one.

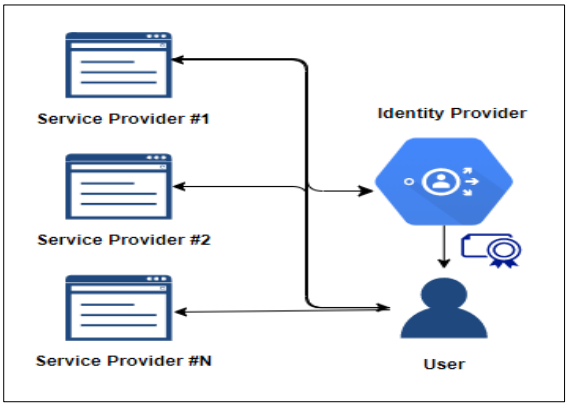

Fig. 3 Federated Identity Model

Towards Decentralized Identity. aims to rectify privacy and data protection concerns by putting the control in the user's hands. The user control is enabled by shifting the transfer of identity information through users, rather than directly between service providers [9].

B. Blockchain

Blockchain technology is a distributed ledger that is widely used for recording distinct transactions. The transactions are maintained by entities on a Peer-to-Peer (P2P) network[10]. Once a consensus is reached among all entities of the network, the transaction is added to a block. All blocks are bound to each other and together formed a Blockchain.

Blockchain involves three basic concepts: block, chain, and transaction. The "block" refers to distributed data. The "chain" refers to the chronological order of blocks placed in the transaction ledger. The "transaction" is the read or write operations on the block for storing and retrieving the data. Fig. 4 shows that the blocks are linked in a chain, so that each block holds the cryptographic hash value of the previous block [9], to give finally the criteria of de-trusted, decentralized, distributed data storage structure. The technology uses cryptographic hashes to ensure that the data of any transaction can't be forged or tampered besides the ability to verification against integrity and security. The distributed nature is served by the distributed data across a network and P2P communication.

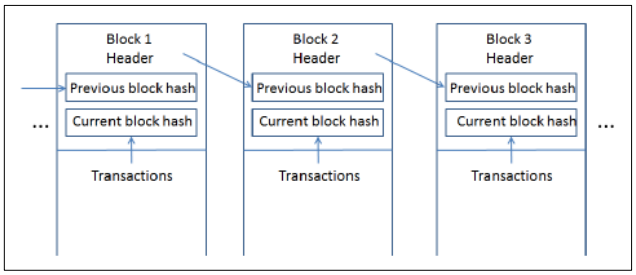

Fig. 4 Simple Blockchain Structure [11].

Most of the appeal toward Blockchain technology revolves around themes associated with its key features:

Decentralization. Any node in the network owns the information and has access to the data stored in Blockchain. This allows network nodes to directly exchange data based on a trusted system. Thus, increasing the efficiency of data exchange and eliminating SPOF [12].

Immutability. Means that once the data has been stored in Blockchain, it cannot be modified [13]. is the cryptographic hash function. Thus restrict all unauthorized changes and hacks in the system and removes the intermediates from the system.

De-trusted. The Blockchain creates linked blocks based on cryptographic hash values and uses digital signatures generated from asymmetric cryptography to ensure the security of transactions [14]. Therefore, the nodes can make transactions safely without third-party control.

Privacy. The user is completely invisible during transmission process because the data are transmitted using public and private keys due to the digital signature algorithm [14].

III. Blockchain-based Identity Management Solutions

According to Dunphy et al. in [15] all distributed ledger technology based IdM proposals fell into one of two categories:

Self-Sovereign Identity. gives the individuals ownership and full control of their identities without the need for identity providers. The provided decentralized identity does not depend on any centralized registered identity provider or certificate authority (CA). Individuals can decide what to share, who to share with, and when to stop sharing their personal data. SSI enables trusted interactions to access individuals' identity information while preserving privacy. This can be enabled by an ecosystem that facilitates the collection and recording of users' attributes. Also, the ecosystem spreads mutual trust between different digital identities. Digital identities can be for institutions, individuals, and devices. Examples include uProt.

Decentralized Trusted Identity. relies on existing trusted credentials such as government identification cards or passports etc. Thus, the proprietary service will be able to perform identity proofing to verify these credentials. Then it stores the identity verification proofs on Blockchain for later validation by third parties. Examples include ShoCard.

We will discuss in detail mainly two solutions, each one belonging to a different category. The first solution is ShoCard which belongs to a decentralized trusted identity model. The second one is uPort which is the first existing identity solution that enables SSI. Furthermore, there are many other Blockchain-based identity systems in the literature, including DNS-IdM which serves online users in general while Health-ID serves patients and remote healthcare providers.

ShoCard [16] is a mobile digital identity that provides identity verification for both online and face-to-face interactions. It utilizes Blockchain to bind between user identifiers, attributes, and existing trusted credentials.

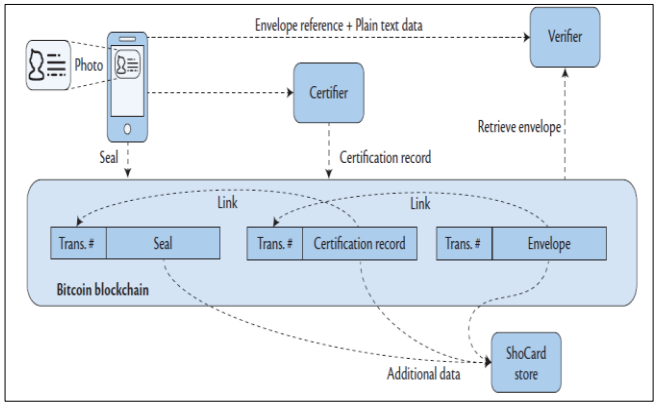

Fig. 5 ShoCard Architecture [15].

Users should first scan their identity credentials using ShoCard mobile application. The trusted credential can be a passport, driving license, etc. The uploaded credentials and the corresponding data are encrypted and kept on the user's mobile device. The signed hash of the user's identity information is added into Bitcoin ledger to be used later for data validation. The resulting Bitcoin transaction number is the user identifier or known as ShoCardID and it is stored on the user's mobile device to be used as a pointer toward the ShoCard seal. In the certification process, the user collects additional attributes from many service providers. Then interacts with an identity provider to associate certificates to his ShoCardID. ShoCard server stores encrypted certifications or known as envelopes to give users the ability to provide their attributes to the relying parties or to retrieve them in case they lose their mobile device. Fig. 5 illustrates the general architecture of ShoCard.

uPort [4] is an open-source decentralized identity framework that provides a digital identity to all internet users to interact with both decentralized applications as well as traditional centralized applications.

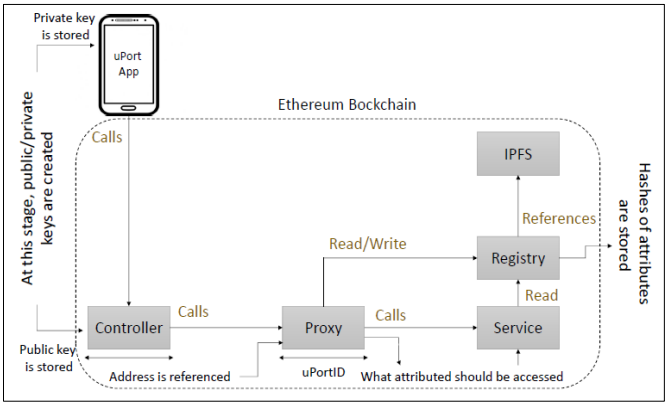

Fig. 6 uPort Architecture [17].

uPort is built on the top of Ethereum ledger and relies on a set of components: smart contracts, developer libraries, and a mobile application. The developer libraries for third-party applications integration. The mobile application for cryptography asymmetric key pair management and for scanning the Quick Response (QR) code to initiate interactions with entities. Users are uniquely identified by a twenty-byte hexadecimal address of the Ethereum smart contract deployed by the user and known as a proxy smart contract. Ethereum smart contracts are the core component of uPort technology. It has four main smart contracts: proxy, controller, recovery quorum, and registry smart contract. The proxy smart contract is used to forward transactions. The controller smart contract is used to maintain control access over the proxy contract. The controller contract consists of user's public key and a list of trusted entities addresses also known as recovery delegates. The recovery quorum smart contract is used to recover user's identity by triggering a vote between recovery delegates listed in the controller contract. When a quorum of delegates is reached within a specific period, meaning more than half of the recovery delegates have been positively voted. Then a new user address is replaced with the lost public key. The new address is connected to a new mobile device. The registry smart contract is used for mapping between uPort identifiers with their associated identity attributes. The attributes are stored off-chain on InterPlanetary File System (IPFS) which is a distributed storage system or on any traditional cloud service such as Microsoft OneDrive and Dropbox. The cryptographic hash of the JavaScript Object Notation (JSON) attribute data is only stored on-chain due to the high cost of large volumes. Fig. 6 illustrates the general architecture of uPort.

DNS-IdM [17] is an IDMS that enables SSI and helps users to maintain their identities with associated attributes. Also, it facilitates the verification process by using real-world identity attribute benefactors. The system is implemented on top of the Ethereum ledger and utilizes smart contracts to secure the management of users' identities.

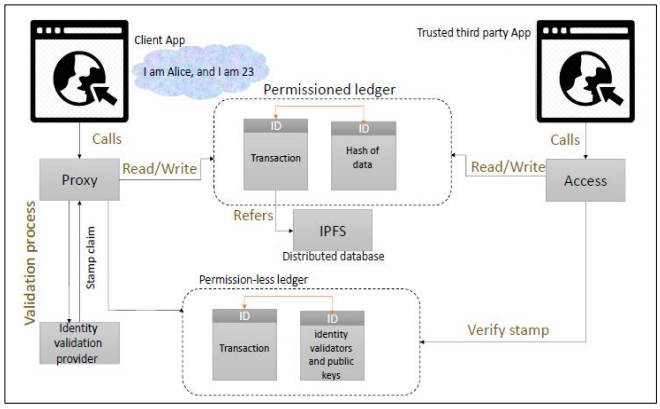

Fig. 7 DNS-IdM Architecture [17].

Users should register first to be able to add their attributes. The attributes itself stored on IPFS, while the hash of attributes and the identification data are stored on a permissioned Blockchain. Attributes are validated before being mined and added to the network. Therefore, DNS smart contract plays its role as a router and redirects to a specialized validation contract based on the type of attributes. The validation contracts and public keys are stored on a permissionless Blockchain. Besides that, the DNS contract grants public access to the entries on a permissionless network. Fig. 7 illustrates the design architecture of DNS-IdM.

Health-ID [18] is a privacy-preserving decentralized IDMS that facilities identification and authentication for both patients and remote healthcare providers across different eHealth domains.

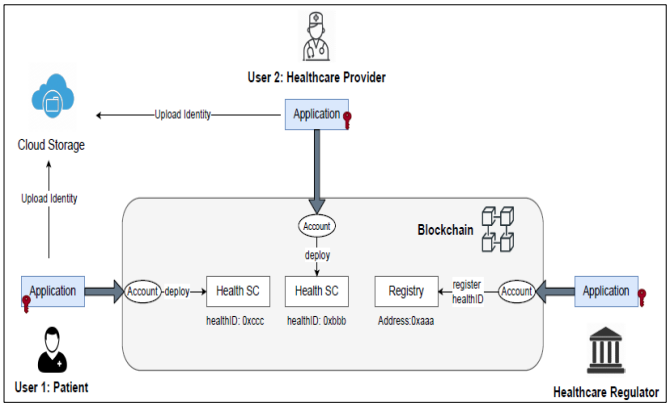

Fig. 8 Health-ID Architecture [18].

There are three participants in the proposed system: regulators, patients, and healthcare providers. The regulators manage the Blockchain. The patients can create, store, and manage their own identity. Healthcare providers can authenticate themself to any patient before providing their health services. The participants will be registered to the Blockchain after performing off-block identity proofing. As a result, the patients and healthcare providers will have a unique identification called healthID which is the address of the smart contract deployed by each entity. The identity attributes are structured in form of a JSON object and then signed by the regulator to create a JSON Web Token (JWT). The owner uploads the encrypted JWT identity attributes over a cloud service (Dropbox, IPFS). The hash of the identity attributes and the hashID which is a unique random number assigned to that hash are further stored on the Blockchain. Fig. 8 illustrates the general architecture of Health-ID.

IV. DISCUSSION

As a conclusion of the above IdM solutions, we carried out an extensive assessment of the solutions. The assessment is divided into three main parts, namely: technology used, identity servers provided, and security-based assessment.

A. *Technology-based Assessment*

Table 2.2 presents a comparison between above IDMS based on the technology used.

Table 1. Comparison between decentralized IdM solutions

Identity Solution	Year	Distributed Ledger	Blockchain Type	Consensus Algorithm	Identity Model
ShoCard	2015	Bitcoin	Permission (less,ed)	≈	Decentralized Trusted
uPort	2016	Ethereum	Permissionless	POW	Self-sovereign
DNS-IdM	2019	Ethereum	Permission (less,ed)	≈	Self-sovereign
Health-ID	2021	Ethereum	Consortium	POA	Self-sovereign

≈Not Addressed

Ethereum platform was used in all discussed IdM solutions except ShoCard which used Bitcoin. Due to the use of the Bitcoin ledger, the transaction confirmation time takes on average ten minutes compared to seconds for Ethereum. As result, the waiting time for ShoCard users will be very high which negatively affects users' experience.

uPort use permissionless Blockchain which is completely open and allows anyone to participate by verifying or adding data to the Blockchain (a process called 'mining') and they are fully decentralized. On the contrary, the permissioned Blockchain that only allows certain authorized entities to participate in a closed network [19]. Thus, a permissioned Blockchain is considered to be centralized but it is faster, more scalable, and transaction fees are extremely low. ShoCard and DNS-IdM get the power of the permissioned and permissionless Blockchain. Health-ID use a consortium Blockhain that considered as hybrid type of blockchain, relies on a set of authorized regulators to manage the network.

Consensus algorithm allows nodes of the Blockchain network to agree on only one version of the truth about the ledger that they hold. uPort uses Proof of Work (POW) that required expensive energy computational to reach a consensus on the state of the ledger. While Health-ID uses Proof of Authority (POA) which is less energy cost than POW and significantly improves transaction throughput.

B. *Identity Services-based Assessment*

Identity provider is the core component of the IDMS, providing users identities and other related identity services namely identity revoke, recovery in case of loss, and IdM such as registration, authentication, and managing users' attributes [6]. all above IDMS provide registration, authentication, and management. Only uPort provides an identity recovery mechanism to recover user identity.

However, none of them enables identity revocation. where revoking an identity means that the entity is no longer participating or interacting in the system.

uPort enables users to recover their identity if their mobile device that's holds the user private key is lost or theft. This allows users to maintain a persistent identifier even in case of lost their keys. However, this mechanism would be vulnerable when the trusted recovery delegates themselves are attackers or malicious entities by replacing the recovery delegate's address list in the controller smart contract with their own identities leads to compromises the user's device key permanently and stealing his identity. Moreover, there is a potential for leakage of attributes in the registry. uPort does not authenticate the owner of the mobile device, meaning if an unauthorized person has access to the user's mobile device, he will have full control of his identity.

Identity proofing is the process of verifying that the user is actually who is claimed to be [20]. This process is required to avoid any identity theft. ShoCard performs identity proofing by canning existing trusted credentials. However, the uploaded credentials may be fraudulent. Also, Health-ID performs off-block identity proofing for healthcare regulators to validate the identity information. After verifying their identity successfully, then healthcare regulators can provide physical or remote identity proofing for patients and healthcare providers. On the other hand, uPort and DNS-IdM do not perform any identity proofing.

C. *Security-based Assessment*

Several distributed IDMS are geared toward taking advantage of intermediaries instead of eliminating them by reshaping their roles. For example, uPort relies on trusted attribute providers and uses a registry that stores the mapping between uPort identifiers with their associated identity attributes. Also, ShoCard uses a central server as an intermediary to manage the exchange of user certifications between users and different relying parties. However, if any security breaches happened or if the company no longer existed, users would be unable to exchange certifications between different relying parties.

Some Blockchain-based IDMS support creating multi-unlinkable identities for the same user. For example, ShoCard, uPort, and DNS-IdM provide creating multiple identities for one user while Health-ID supports only a single identity for the user.

V. CONCLUSION

The great properties of Blockchain technology as a decentralized and incorruptible database, the great success in virtual currencies, and the availability of the Internet have opened up great new opportunities to use this technology in IdM to deal with user privacy protection. In recent years, there have been attempts to develop Blockchain solutions for the next generation of IDMS, which allow users to have full control of their own identity. This paper reviewed the principles of IdM and Blockchain and discussed the main IdM models and highlights their advantages and drawbacks. Also, this paper explored in-depth the recent IDMS that enable decentralized identity: ShoCard, uPort, DNS-IdM, and Health-ID by describing their architecture, components, and their interaction. Finally, a comparative assessment is presented for all discussed IDMS. It was observed that blockchain is suitable to overcome some limitations of conventional IDMS. Nevertheless, it is still lacking in the published studies in the area of IdM.

REFERENCES

[1] 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*. King Saud bin Abdulaziz University, 2021. doi: 10.1016/j.jksuci.2021.03.005.

[2] M. Shuaib *et al.*, "Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison," *Mobile Information Systems*, vol. 2022. Hindawi Limited, 2022. doi: 10.1155/2022/8930472.

[3] B. Faber, G. Michelet, N. Weidmann, R. Rao Mukkamala, and R. Vatrapu, *BPDIMS:A Blockchain-based Personal Data and Identity Management System*. [Online]. Available: https://hdl.handle.net/10125/60121

[4] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, "UPORT: A PLATFORM FOR SELF-SOVEREIGN IDENTITY," 2016. Accessed: May 26, 2022. [Online]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf

[5] M. K. Hamza, H. Abubakar, and Y. M. Danlami, "Identity and Access Management System: a Web-Based Approach for an Enterprise," *Path of Science*, vol. 4, no. 11, pp. 2001–2011, Nov. 2018, doi: 10.22178/pos.40-1.

[6] 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. Academic Press, Sep. 15, 2020. doi: 10.1016/j.jnca.2020.102731.

[7] N. Chaudhry and M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities," in *2018 International Conference on Open Source Systems and Technologies (ICOSST)*, 2018.

[8] G. T. Nguyen and K. Kim, "A survey about consensus algorithms used in Blockchain," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 101–128, 2018, doi: 10.3745/JIPS.01.0024.

[9] O. Dib and K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions," *Annals of Emerging Technologies in Computing*, vol. 4, no. 5. International Association for Educators and Researchers (IAER), pp. 19–40, 2020. doi: 10.33166/AETIC.2020.05.002.

[10] R. Al-Amri, N. H. Zakaria, A. Habbal, and S. Hassan, "Cryptocurrency adoption: current stage, opportunities, and open challenges," *International Journal of Advanced Computer Research*, vol. 9, no. 44, pp. 293–307, Sep. 2019, doi: 10.19101/ijacr.pid43.

[11] J. Pan, Y. Liu, J. Wang, and A. Hester, "Key Enabling Technologies for Secure and Scalable Future Fog-IoT Architecture: A Survey," Jun. 2018, [Online]. Available: http://arxiv.org/abs/1806.06188

[12] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, Feb. 2020, doi: 10.1016/j.jisa.2019.102407.

[13] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 61048–61073, 2021. doi: 10.1109/ACCESS.2021.3072849.

[14] H. Sun, X. Wang, and X. Wang, "Application of blockchain technology in online education," *International Journal of Emerging Technologies in Learning*, vol. 13, no. 10, pp. 252–259, 2018, doi: 10.3991/ijet.v13i10.9455.

[15] 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.

[16] "ShoCard." https://www.shocard.com/en.html (accessed May 26, 2022).

[17] J. A. 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 (Switzerland)*, vol. 9, no. 15, 2019, doi: 10.3390/app9152953.

[18] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-id: A blockchain-based decentralized identity management for remote healthcare," *Healthcare (Switzerland)*, vol. 9, no. 6, Jun. 2021, doi: 10.3390/healthcare9060712.

[19] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "BSDCE-IoV: Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3265959.

[20] M. Shimaoka and N. Sonehara, "Modeling the cost structure of identity proofing," in *Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014*, Institute of Electrical and Electronics Engineers Inc., Sep. 2014, pp. 180–185. doi: 10.1109/COMPSACW.2014.34.