RESEARCH ARTICLE OPEN ACCESS

Blockchain based Identity Management System: A Survey

C. Victoria Priscilla*, T. Devasena**
***(*Department of Computer Science, SDNB Vaishnava College for Women,*
University of Madras, Chennai, India
***** (*Department of Computer Science, SDNB Vaishnava College for Women,*
University of Madras, Chennai, India

ABSTRACT
Reliable identity management system is an integral part of the enterprise. Blockchain is a distributed ledger that is decentralized, cryptographically signed, with the ability to solve the protection and privacy problems of Centralized Identity Management System. The distributed consensus design of the blockchain will prevent malicious attacks, and enables self-sovereign identity by providing an individual to have more control over their information and to share minimum amount of information that are required for identification. This paper focused on the leveraging power of Blockchain technology in Digital Identity Management.

Keywords – Blockchain, Consensus, Identity Management System, Zero knowledge proof

Date of Submission: 12-05-2021 Date of Acceptance: 25-05-2021

I. INTRODUCTION

This literature review focused on the blockchain technology identity management system. This review includes the analysis of existing research papers, journals, news papers articles, academic books and industrial reports. This paper focused on how the blockchain technology used to create a zero-knowledge identity for each citizen. It also focused on Digital Identity management that streamlining the service provided by the nation.

The Identity Management System (IdM) refers to the framework that involves the management of individual digital identities, their authentication, and authorization across enterprise with the goal of increasing security. The digital identities that include personal identity of a citizen are not only expected to be authenticated but also tamper proof as nowadays data are the honey pot for criminals. The list of personal information can be pretty expensive. They should be protected with super tight security system. To obtain any government services like LPG connection, opening a bank account and getting a SIM card, at every point government authorized ID's like Aadhaar card, Voter ID, PAN card, Passport etc are very important. The present identity management system stores personal identification of all citizens in a centralized Identity Management system. Centralized Identity Management system follows client - server architecture, where all the information are stored in a centralized server and one or more client directly connected to the central server. The major challenges of using centralized Identity management system are Identity theft and lack of control.

For hackers, data breaches are a gold mine. One such example for centralized identity management system is UIDAI (Unique Identification Authority of India) Called Aadhaar verification service. Aadhaar authentication is that the process wherein Aadhaar number, alongside other attributes, including biometrics, are submitted online to the Central Identities Data Repository (CIDR). Since CIDR is the centralized system it is important to examine its security issues. Even though the government claims of biometrics data and the enrolment process of UIDAI being more secured with its database in a central server with super tight security and protected by best in class cryptography, UIDAI fall short[1]. "The security flaws of Aadhaar can have devastating implications for Indians" is stated in an article published by the Business Standard [2] and if it is left unaddressed then Aadhaar will be the largest, leakiest database in the world [3].The Economic Times also published an article [4] that " In order to implement data security and ensure that no person's data is used against him, there must also be an independent oversight body". And the blockchain technology that stores information in a distributed database may be a solution to these kinds of issues.

The rest of this paper is structured as follows. The following Sect.2 introduces blockchain architecture and different types of blockchains and their use-cases. Sect.3 shows typical consensus algorithms used in blockchain technology. Sect.4 discusses the problems encountered by the

Centralized Identity Management System and the leveraging power of Blockchain Technology in digital identity management systems, Sect.5 Summarizes the Systematic Review Results. Finally, Sect.6 concludes the paper.

II. BLOCKCHAIN TECHNOLOGY

Blockchain technology is a Distributed Ledger Technology (DLT) consisting of decentralized databases that, using consensus algorithms, provide control over data between entities via a peer-to-peer network. A blockchain is a series of time stamped transactions, where a variable number of output addresses (each address is a 160-bit number) is used in each transaction[2].

2.1 Blockchain Architecture

Blockchain is a distributed peer-to-peer network where non-trusting members can verifiably interact with each without the need for a trusted authority[3]. Blockchains are cryptographically signed digital ledgers where transactions are framed into blocks. Each blockis linked to previous block with its hash value which is generated cryptographically, as illustrated in Fig.1. The first block of the blockchain is called genesis block and each block is having only one parent block. When new blocks are added, it is reflected across all copies of the ledger in the network. If any slight changes in the block, the hash value of that block changes drastically, this will result in the breaking of chain into subsequent block[4].

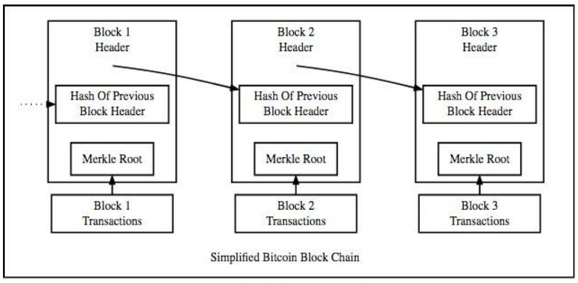

Fig1. Blockchain Architecture

Blockchain technology is a type of open cryptography that, together with a publicly accessible repository that is controlled in an automated and decentralized manner, uses public and private keys to protect information. When encrypted, you need both the pass code and the private key to decrypt the information making it possible for all the encrypted data to be taken and yet be completely worthless to the third party.

2.2 Types of Blockchains

There are four major types of Blockchain networks.

- Public blockchains
- Private blockchains
- Consortium blockchains
- Hybrid blockchains

1) *Public blockchain:* A public blockchain is also known as permission less distributed ledger system. It has absolutely no limits on entry. If they have a network, everyone can enter and access the public blockchain. The bitcoin blockchain and the Ethereum blockchain are the first public blockchains. It made it possible to do transactions in a decentralized way for everyone linked to the internet. Proof of Stake(PoS) or Proof of work (PoW) [5][6] are the consensus algorithms used to validate a transaction in public blockchains.

2) *Private Blockchain:* A private blockchain is a blockchain operational restrictive or permission blockchain operative only in a closed network. In a corporation or company where only selected members are members of a blockchain network, private blockchains are commonly used. It varies only in the way it is accessed from the public blockchain; otherwise, it provides the same collection of features as that of the public blockchain. For voting, supply chain management, digital identity, asset ownership, etc., private blockchain networks are deployed [5][7].

3) *Hybrid blockchain:* A hybrid blockchain may be a mixture of a blockchain that is private and public. It uses the functionality of both types of blockchains and can also be used as a public permission-less framework for a personal permission-based system. Users will monitor who gets access to which data is stored inside the blockchain in such a hybrid network. Only a chosen portion of blockchain data or documents may be permitted to go public in the private network [6][7] , keeping the rest confidential.

4) *Federated blockchain / Consortium blockchain:* A consortium blockchain is a semi-decentralized form where a blockchain network is managed by more than one organization. This is contrary to what we have seen in a private blockchain that is operated Only by a single entity. Usually, consortium blockchains are used by banks, government organizations, etc [6].

Table1. Comparison between Public, Private, and Federated Blockchains

	Public	**Private**	**Consortium**
Type	Open and Decentralized	Controlled and Restricted	Controlled and Restricted
Participants (Identity)	Permissionless Anonymous, Pseudonymous -Could be malicious	Permissioned -Identified -Trusted	Permissioned -Identified -Trusted
Consensus Mechanisms	Proof of Work, Proof of Stake, Proof of Authority, Proof of Elapsed Time etc., -Large energy consumption -No finality -51% attack	Voting or multi-party consensus algorithm -lighter -Faster -Low energy consumption -Enable finality	Voting or multi-party consensus algorithm -lighter -Faster -Low energy consumption -Enable finality
Transaction Approval Frequency	Long Bitcoin: 10 min or more	Short 100 x msec	Short 100 x msec
Example of Blockchain	Bitcoin, Ethereum, Litecoin etc	Multichain, Hyperledger Fabric, Hyperledger Sawtooth, Corda	R3(Bank), EWF-Energy B3i-Insurance
Use-Cases	Voting, Fundraising	Supply chain management, Asset ownership, Internal Voting	Banking and payments, Research, Food tracking

III. CONSENSUS ALGORITHMS

A consensus algorithm is a computer science method that is used between distributed processes or systems to achieve agreement on one data value. Consensus algorithms are intended to achieve reliability in a network that involves many unreliable nodes[8]. Table2. describes different types of Consensus Algorithm and their Characteristics.

Proof of Work The Proof of Work Proof of Work (POW) is a common consensus algorithm used by bitcoin and litecoin [8], most successful cryptocurrency networks. It requires some node in the blockchain network has to be selected to add a new block in to the network. As random selection of node is vulnerable to attacks, the node that wants to publish a block in the network has to do some computing work[9], usually it is a complex mathematical puzzle. It requires huge computational power and energy consumption.

Proof of Stake Another popular consensus algorithm, Proof of Stake (POS), has emerged as a low-cost, low-energy alternative to the POW algorithm [8]. To select a node to be the evaluator of the next block, PoS is a pseudo random election procedure. Node selection is based on the variables that include staking age, randomization and wealth of nodes. The richest node will be less likely to strike the network because the election is focused on the account balance[9].

practical Byzantine Fault Tolerance (pBFT) algorithm was proposed by C. Miguel et.al. This deals with creating a Byzantine fault tolerant system. The distributed system allowed by pBFT is ordered sequentially with one node being the primary (or leader node) and others identified as secondary (or the backup nodes). In spite of malicious nodes in the system failing or sending out incorrect information[10], it helps the system to reach a consensus. A practical Byzantine Fault Tolerant system will operate as long as the maximum number of malicious nodes in the system must not be greater than or equal to one-third of all nodes. The system becomes more secure [9] as the number of nodes increases.

Delegated Proof of Stake a further enhancement to the standard Proof of Stake algorithm is the Delegated Proof of Stake. It is used for consensus within the BitShares network [9].DPoS is a representative democratic, in which the users can either directly vote or giving their voting power to another entity to vote on behalf of them. Selected witnesses are responsible for creating blocks by verifying transactions.

The alteration of the earlier applications is *Proof of Activity, Proof of Burn* and *Proof of Elapsed Time.*

IV. DIGITAL IDENTITY MANAGEMENT ANDTHE POWER OF BLOCKCHAIN

Identity Management system is a digital identity system[11] which enable the user to manage storage, authentication, authorization, data sharing and protection of identities within the organization

Table 2. Comparison Between Consensus Algorithms

Consensus Algorithm	**Characteristics**					
	Blockchain type	**Transaction Rate**	**Scalability of Net work**	**Adversary Tolerance**	**Energy Requirements**	**Typical Examples**
Proof of Work (PoW)	Permission less	Low	High	<25% of computing power	High	Bitcoin / Litecoin / Ethereum (until 2018)
Proof of Stake (PoS)	Both	High	High	<51%of stake	Medium	Tendermint/ Ethereum (from 2018)
Delegated Proof of Stake(DPoS)	Both	High	Medium	<51%of validators	Low	BitShares / EOS / Lisk / Ark / Steem
Byzantine Fault Tolerance (BFT)	Both	High	Medium	<33.3% of faulty replicas	Low	Practical BFT (SIEVE & XFT) / Federated BFT (Stellar & Ripple)

and on the web. The digital identity is important aspect of online financial transactions. Nowadays, digital identity management system plays a vital role in providing various services to the citizens by the government. Singapore, for example, has developed the National Digital Identity (NDI) system as part of its Smart Nation Initiative, which is expected to help people securely access e-government services. India has also created the Aadhaar ID, a single digital identity linked to all social schemes, which has changed the way subsidies are distributed to economically disadvantaged groups. These kinds of national identities usually contain the name, citizenship, date of birth, and a national identifier. Hence, it is important to have a robust identity management system to secure the data from being tampered with. The currently deployed system is susceptible to single point failure, lack of interoperability and privacy issues[12]. The blockchain based IDMSs ensures the consensus, transparency and integrity of the personal data sharing on distributed ledger technology(DLT)[13].

The present-day centralized Identity management system encounters several problems like single point of failure, identity theft, data control issues, external and internal data breaches. The aggregation of personal information in one centralized database brought back concerns about privacy and security. The Servers can be hacked, and the accumulation of personal data in the possession of a limited number of organizations raises the possibility of further breaches. Blockchain solves these problems with transparency, security, authenticity and enables the user to gain control over their personal data.

In Fig2. Blockchain Identity management system, the personal data were not stored in the blockchain instead they were stored in IPFS (Inter Planetary File System) and it uses smart contracts to enable controlled data disclosure. Thus, it is not possible to manipulate the data on the blockchain. Since the system will be decentralized, there will be no single point of failure. Thus, by using blockchain one can create self-sovereign and encrypted digital identities.

In Fig2. The public distributed ledger works using a hashing encryption. Every block has a hash value, which is used as the digital signature of the block. These hash values are generated by smart contracts which are simple programs that run when predetermined conditions are met. They're usually used to simplify the execution of an agreement so that both parties can be confident of the result right away, without the need for any intermediaries or time waste. A consensus algorithm is used to authorize and verify all transactions on the Blockchain network.

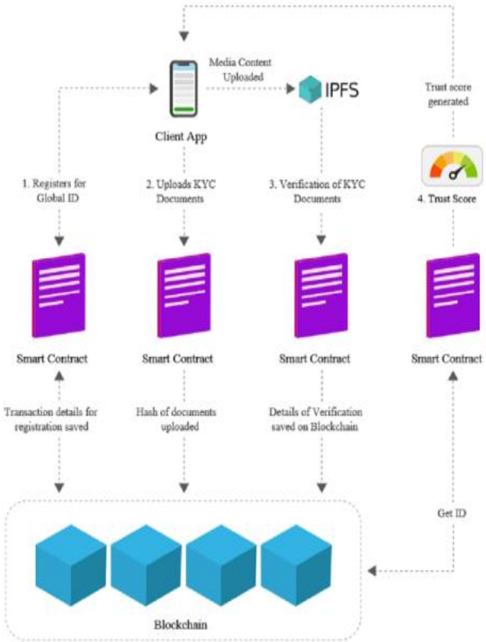
Media Content Uploaded
IPFS
Trust score generated
Client App
1. Registers for Global ID
2. Uploads KYC Documents
3. Verification of KYC Documents
4. Trust Score
Smart Contract
Smart Contract
Smart Contract
Smart Contract
Transaction details for registration saved
Hash of documents uploaded
Details of Verification saved on Blockchain
Get ID
Blockchain

Fig2. Block chain Identity Management System

A few real life samples of how blockchain technology is getting used for Digital Identity Management are:

- Since 2012, blockchain has been used in Estonia, both in the public and private sectors, to preserve national data and services. Estonia manages the blockchain multipurpose digital ID card [17] and ensures that all data changes are detected instantly based audit trails left by the "digital defense dust" that covers it.
- The city of Zug [18] in Switzerland is exploring an identity issued by a self-sovereign government on Ethereum using uPort, providing easy and safe access to a suite of e-government services. This removes the need to access government facilities with a user ID/password.
- ID2020 [19] is a global coalition to accelerate the process of granting digital identity to those who are 'invisible' to society through states, public, private and non-governmental organizations. Blockchain-based technologies and interoperability across different geographies and reuse/integration/connectivity with current systems are being carried out to meet this objective.
- The Verifiable Organizations Network (VON) on the Sovrin blockchain in the provinces of British Columbia and Ontario in Canada .[15]
- Travelers scan their passports through a Smartphone app and take selfies, using a private key to hash this authentication information on the blockchain, ShoCard/SITA method .[19]

The advantages of distributed digital identity system using blockchain over the centralized identity system are:

- Integrity: As the data is distributed across the peer-to-peer networks, it is constantly reconciled, as well as being kept up to date. Furthermore, the blockchain network has no single point of failure, making it impossible for hackers to compromise the data set's integrity.
- Simplicity: The blockchain framework automates the issuance of digital identity and simplifies the process of on-boarding customer and data verification.
- Privacy: The blockchain protects citizens' confidential and sensitive information by encrypting it and using a digital signature to provide evidence of a transaction. The potential benefits of blockchain based identity management system to personal digital identity are summarized in the following Table3.

Table3. Benefits of Blockchain Based Identity Management System

Zero Knowledge proof	A blockchain-based identity management system can be used to verify a user's identity without disclosing personal information.
Secure	Blockchain limits data access capability to only authorized persons which helps to prevent unauthorized access to personal and confidential data.
Faster & efficient	Since user identities are provided and validated on the Blockchain network, additional time for identity verification prior to user on-boarding is avoided.
Reduce cost	Managing and verifying a user's identity on blockchain eliminates the need for an external provider for identity authentication, resulting in significant cost savings.
Trust and Transparency	The Blockchain verifies and issues identities on a decentralized ledger that is open to all on the same network. It contributes to the data in the system becoming more trustworthy and transparent.
Distributed	As per Blockchain inbuilt capability all the data is distributed to all the participants of the network and helps to avoid any conflicts.
Eliminate identity theft	As users personal data is in the control of user only and stored in the form of cryptographic hash. It helps to eliminate any theft respective to user's identity data.
Unique identifier	By managing identity on Blockchain and bringing other identity provider and issuer on the same platform helps to manage single and unique identity.

ZERO KNOWLEDGE PROOF

A zero-knowledge proof (ZKP) is a cryptographic method that allows one individual (the prover) to persuade another individual (the verifier) that they need to provide some data without disclosing the information to the verifier [17]. Shafi Goldwasser, Silvio Micali, and Charles Rackoff first developed zero-knowledge evidence in their paper

"The Knowledge Complexity of Interactive Proof-Systems" in 1985 [18].

A Zero-Knowledge Proof is an authentication technique that enables one entity to prove to another entity by the use of cryptography that it knows certain information or meets a certain criteria without having to reveal any of the real information that supports that evidence [19]. Therefore, the person checking the evidence has "zero knowledge" of the facts supporting the evidence, but is "convinced" of its validity. This is particularly useful when and where the prover entity does not trust the verifying entity but also has to prove to them that the prover entity knows relevant information [20]. This allows a person to prove that their personal data meet certain criteria in an identity management with blockchain scenario without disclosing the actual details.

V. RESULTS

The outcome of the mapping study will allow us to identify and map the cases of blockchain usage in digital data management and to understand the applications based on blockchain. Since there are several use-cases for blockchain in various industries with its ability to build transparency, and fairness in saving business time and money, in this paper the use-cases which are relevant to securing personal data in various sectors are taken into consideration. The following table gives the summary of those identified use cases and their example applications.

Table 3. Use Cases And Example Applications

Use cases	**References**	**Example Applications**
Healthcare	[4][14]	Health Nexus ,MedRec, ConnectingCare
Electronic Voting	[15][16][3]	Voatz, Votem,Smartmatic-Cybernetica
Personal identity Security	[1][17][15]	Civic, Evernym, Ocular
Identity Management	[12][18][19][20][21][22][11]	Uport, Sovrin, Shocard
Cyber security	[2][23][11]	KYC(Know your Customer), Cryptocurrencies, Coinbase

This paper finds it is important to discuss the Consensus Algorithm of Blockchain Technology. The following Table4. demonstrates the Consensus algorithm used in the selected Papers, their usage frequencies, advantages and disadvantages of each consensus algorithms. It is also interesting to observe that most of these applications uses Proof of Work algorithm to bring consensus on the blockchain distributed network.

Table4. Usage Frequency Of Consensus Algorithm In Blockchain Based Idms

Consensus Algorithm	**Usage Freq.**	**Ref.**	**Advantage**	**Disadv.**
Proof of Work (PoW)	4	[17] [15] [22][2]	Highly scalable, suitable for variety of applications .	Energy consumption, Costly, vulnerable to 51% attack
Proof of Stake (PoS)	1	[23]	Higher speed, less Energy consumption, less hardware requirement	Vulnerable, Unbalanced / inherent inequality (the richest can have control of the consensus.
Elliptic Curve Signature Algorithm (ECDSA)	2	[22] [18]	Smaller keys, Moderately fast encryption, Fast signatures.	Complicated and tricky to implement, Newer algorithms have unknown weakness.
Byzantine Fault tolerance	1	[2]	Energy efficiency, Transaction finality	Sybil attacks, scaling

In Fig3. The usage Frequency of Consensus algorithms of blockchain technology based on identity management system has been shown. And it is important to note that Proof of work consensus algorithm found more usage frequency over other consensus algorithms, it can be assumed that this is because of their high scalability and frequent usage in most popular blockchain applications.

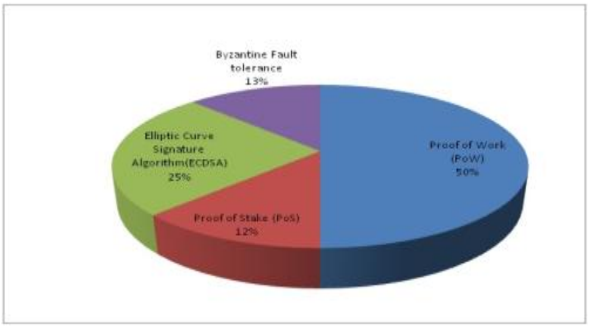

Fig3. Usage Frequency of consensus algorithms

In this survey the digital identity management and the leveraging power of blockchain technology has been explored. Nevertheless, every system has its own challenges and trade-offs Blockchain identity management system is also having its own pros and cons. In this session few challenges of Blockchain Identify management system are discussed as follows.

- Scalability: Blockchains are not scalable as that of centralized system. It is related to the blockchain network issues. If more people or nodes enter the network the greater the chances of it slowing down.
- High energy Consumption: From this survey, as shown in Fig.3 it is very clear that the proof of work consensus algorithm found more common in all the blockchain based applications. In Proof of Work algorithm, the miners are required to solve most complex mathematical problem. The high energy consumption to solve these complex mathematical problems makes it not so ideal for real-world.
- Data Immutability: It is obvious that Blockchain benefits a variety of structures, including supply chains, financial systems, and so on. Blockchain network evenly distributed among all the nodes. If a person owns 50% or more of the nodes in a blockchain network, making it vulnerable.
- Maturity: Blockchain has only been around for a decade. This indicates it is a modern technology that it will take some time to develop. Considering various consortiums to solve the decentralized problem is the unique solution.

VI. CONCLUSION

While blockchain applications are being widely deployed, many issues have yet to be addressed. Through doing so, blockchains would not only become more flexible and powerful, but also more robust. Since the decentralized, distributed public ledger Blockchain plays an important role in the digital identity management system, it is important to remember that it is not a solution for all identity management difficulties. It also has its own pros and cons, like any device. Many organizations and nations are joining together to ensure interoperability across their boundaries, taking advantage of the benefits of transparency and trust offered by blockchain frameworks. Continuous technological progress and knowledge will contribute significantly to reducing risk and helping us move to a safer planet.

REFERENCES

[1] M. J. Casey, “Signature Signature Ml ~ ibmraes,” 2018.

[2] G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” *Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015*, pp. 180–184, 2015, doi: 10.1109/SPW.2015.27.

[3] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telemat. Informatics*, vol. 36, no. November 2018, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.

[4] C. Agbo, Q. Mahmoud, and J. Eklund, “Blockchain Technology in Healthcare: A Systematic Review,” *Healthcare*, vol. 7, no. 2, p. 56, 2019, doi: 10.3390/healthcare7020056.

[5] “Exploring the different types of blockchain | by The Modex Team | modex_tech.” https://blog.modex.tech/exploring-the-different-types-of-blockchain-10395da93a51 (accessed Sep. 22, 2020).

[6] “4 Different Types of Blockchain Technology & Networks | 101 Blockchains.” https://101blockchains.com/types-of-blockchain/ (accessed Sep. 19, 2020).

[7] “Types of Blockchains - Decide which one is better for your Investment Needs - DataFlair.” https://data-flair.training/blogs/types-of-blockchain/ (accessed Sep. 19, 2020).

[8] “Consensus Mechanism (Cryptocurrency) Definition.” https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp (accessed Sep. 22, 2020).

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[10] V. Lai, “What is Practical Byzantine Fault Tolerance (pBFT)? - Crush Crypto,” *Blockonomi*, 2018, [Online]. Available: https://blockonomi.com/practical-byzantine-fault-tolerance/%0Ahttps://crushcrypto.com/what-is-practical-byzantine-fault-tolerance/.

[11] R. Nechushtai, M. Elit, and S. M. Systems, “Blockchain Identity Management System Based on Public Dentities Ledger,” *Google Patents*, vol. 1, no. 12, 2017, [Online]. Available: https://patents.google.com/patent/US9635000B1/en.

[12] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems,” 2019, doi: 10.6028/NIST.CSWP.07092019-draft.

[13] 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, 2018, doi: 10.1109/MSP.2018.3111247.

[14] R. Surya and G. C. P. Latha, "Blockchain: A panacea for healthcare cloud -based data security and privacy," *Test Eng. Manag.*, vol. 82, no. February, pp. 6671–6676, 2020.

[15] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," *2nd Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2020 - Conf. Proc.*, no. Icimia, pp. 71–75, 2020, doi: 10.1109/ICIMIA48430.2020.9074942.

[16] H. F. Atlam and G. B. Wills, *Technical aspects of blockchain and IoT*, 1st ed., vol. 115, no. January 2019. Elsevier Inc., 2019.

[17] S. P.J and G. George, "Blockchain Based Aadhaar Security," *Int. J. Eng. Technol.*, vol. 7, no. 4.6, p. 398, 2018, doi: 10.14419/ijet.v7i4.6.28450.

[18] 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," *Appl. Sci.*, vol. 9, no. 15, 2019, doi: 10.3390/app9152953.

[19] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, and S. Wang, "c," *Proc. - 2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017*, pp. 44–53, 2018, doi: 10.1109/PST.2017.00016.

[20] O. Jacobovitz, "Blockchain for identity management," *Tech. Rep. Ben-Gurion Univ.*, no. 1, pp. 1–19, 2016, [Online]. Available: https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf.

[21] X. Zhu and Y. Badr, "Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions," *Sensors (Basel).*, vol. 18, no. 12, pp. 1–18, 2018, doi: 10.3390/s18124215.

[22] P. Alto, P. Alto, P. Alto, and R. U. S. A. Data, "[Patent]Identity management service using a blockchain providing certifying transactions between devices," vol. 2, no. 12, 2017.

[23] K. Mudliar and H. Parekh, "A comprehensive integration of national identity with blockchain technology," *Proc. - 2018 Int. Conf. Commun. Inf. Comput. Technol. ICCICT 2018*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICCICT.2018.8325891.