International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 07, ISSN No. 2455-2143, Pages 38-45
Published Online November 2023 in IJEAST (http://www.ijeast.com)

IDENTITY MANAGEMENT, SSI AND BLOCKCHAIN: A REVIEW

Vivek Gujar
Director
IndoAI Technologies P Ltd, Pune, Maharashtra, Pune

Abstract— **As an individual, in the social and digital world, the burden of managing multiple online IDs and passwords, while handling a host of documents e.g passports, driver's licenses, Social Security/Aadhar cards and medical insurance cards is cumbersome. Identities both in the social and digital world requires security and privacy: managing these identities efficiently is called Identity Management. Once these identities established, they are produced, shown, send, verified in some way or the other for various processes in Government and non-Government purposes. Lately it is established that Blockchain technology has immense use to control over identities (Identity Management) with complete secrecy and privacy. Self-sovereign identity (SSI) is undergoing a transformative evolution, driven by the integration of blockchain technology and Facial Recognition Technology (FRT). This envisioned future entails a paradigm shift where unique facial features serve as the secure key for unlocking one's identity. Blockchain, functioning as a decentralized and secure repository, facilitates the storage of facial data. This convergence of SSI, blockchain, and FRT not only augments security but also streamlines authentication processes, reducing the reliance on conventional passwords and identification documents. It's a future where individuals can seamlessly access their data, marking a significant advancement in secure and personalized identity management within an academic context.**

Keywords— **Identity Management, Blockchain, ZKP, DLT, SSI, Facial Recognition Technology, Indoai**

I. INDENTITY MANAGEMENT

Identity management (IdM), also known as Identity and Access Management (IAM or IdAM), is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. The terms "identity management" (IdM) and "identity and access management" are used interchangeably in the area of identity access management [1]. IT security and data management drives and control IdAM. Identity and access management systems not only identify, authenticate and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees need to access. Identity and access management solutions have become more prevalent and critical in recent years as regulatory compliance requirements have become increasingly more rigorous and complex. This identity is essentially a digital identity as it is going through some software and hardware process[2].

Singh et al [3] define term "Identity Access Management" ensures the job identities and nature of the right people c easily accessed through relevant tools. The framework includes different processes, policies, and technologies to monitor user access and manage digital identities. Identity management is needed to improve data security, control user data access, and maintain distance from illegal access.

Devi et al 's [4]Identity management includes maintaining the data used for identity and their access control. A Holder, an Issuer, and a Verifier are the three key actors in the Identity management system. The Digital Identity management provides the ownership of data to the user to promote full user control and transparency is also achieved.

According to Wikipedia a digital identity is information on an entity, used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. ISO/IEC 24760-1 defines identity as "set of attributes related to an entity."

Digital Identification is unique to an individual, having special attributes/properties. Using these set of digital information, it ensures same level of confidence that a face-to-face transaction would happen, and are stored in databases and differentiate users from each other within the same system. A digital identity can be assigned to an individual, a legal entity or companies and even assets.

The International Telecommunications Union[5] defines Digital Identity as "a digital representation of the information known about a specific individual, group or organization". Digital identity consists of all of the individual's personal data that is available online. It can be all encompassing — not just an e-mail or physical address, but also pictures, bank account information and now it is in both forms: offline and online.

In the early 1990s, the authentication method based on username and password was commonly used by individuals during an access process, with a management of dozens of identities as a result of the registration into several Service Providers. Consumers are increasingly adopting digital

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 07, ISSN No. 2455-2143, Pages 38-45
Published Online November 2023 in IJEAST (http://www.ijeast.com)

identity for online transactions—both for buying goods and services as well for banking—and across multiple devices.

1.1 Importance of Indentity Management

One of the purposes of issuing digital identities is that the holders are able to authenticate themselves at the point of service delivery. Authentication happens in any of the following ways (or a combination of these): 'What I know', 'What I have' and 'What I am'. 'What I know' will include things like username, password or PIN; 'What I have' will include factors like possession of a smart card; and 'What I am' will include biometrics (like fingerprint or iris scan). Typically, two-factor authentication is used for various transactions – for example, the use of a card along with PIN for a debit/credit card transaction[5]. Digital Identity fulfils a crucial role in financial transaction while expediting the customer on-boarding process (KYC) primarily preventing Anti Money Laundering (AML) and other fraudulent activities.

Digital identity Management aims to standardize and streamline citizen services provided by nations. Companies are going to spend over $100 billion on cybersecurity this year to fortify their systems to be as strong as Fort Knox, but without a strong Identity Access Management strategy, they could be building a very strong fortress while forgetting to lock the door[6]. At the current rate of growth, damage from cyberattacks will amount to about $10.5 trillion annually by 2025—a 300 percent increase from 2015 levels [7].

1.2 The problems with current Indentity Management systems

Identity has a problem. If it's paper-based, such as birth certificates, it is subjected to loss, theft or fraud. As such digital identity is a plug-in for greater interoperability within government departments reducing bureaucracy. Traditionally this digital identity is stored on a centralised server so it is a honeypot for hackers. Since 2017 alone, more than 600 million personal details – such as addresses or credit card numbers – have been hacked, leaked or breached from organisations. Every six months we hear breach or compromising in system. So it could be premised that most of the current identity management systems are weak. One of reason given is budget constraints. Identities need to be portable and verifiable everywhere, any time, and digitization can enable that. But being digital is not enough. Identities also need to be private and secure.

Several industries suffer the problems of current identity management systems[8]:

- Government: The lack of interoperability among government departments and across different government levels results in excessive bureaucracy, leading to prolonged processes and increased costs.
- Healthcare: Approximately half of the global population lacks access to quality healthcare. The absence of interoperability among various healthcare stakeholders, including hospitals, clinics, insurance companies, doctors, and pharmacies, contributes to inefficiencies in healthcare delivery, causing delays in care and frustration for patients.
- Education: An estimated two hundred thousand counterfeit academic certificates are sold annually in the United States alone. The challenge of verifying the authenticity of these credentials leads to the hiring of unqualified professionals, causing damage to the reputations of universities and the companies that hire them.
- Banking: The requirement for login details, such as passwords, diminishes the security of banking for users.
- Businesses in General: The current necessity to store personal data of clients and employees poses a liability for companies. A breach of personal data may result in substantial fines due to GDPR violations, as seen in cases like British Airways, or lead to a loss of customer trust and subsequent damage to the organization's brand.

Present identity management systems face challenges related to privacy and security. Blockchain technology emerges as a potential solution to address these issues. In the following discussion, we will explore the concept of blockchain, its advantages in comparison to identity management, and delve into the roles played by cryptography, zero-knowledge proofs, and Self-Sovereign Identity.

II. BLOCKCHAIN TECHNOLOGY

Shivshankar [9] defines blockchain as a distributed database that is shared by nodes on a computer network. A blockchain functions as a database, storing information in an electronic format. Distributed Ledger Technology (DLT), commonly simply called "Blockchain Technology", build on consensus mechanism that ensure replication across the nodes of the network ie all the nodes get same information and change of information is noted by every node. If all the nodes agree then the change is accepted [10]. In a financial transaction book, ledger, where the accountant records is available with all the users. If someone records a transaction it is reflected/seen by all the users simultaneously and it would be there forever, and at the real time, would be cross-referenced to check whether what was written to be valid and true; this is the essence of DLT. So, the transaction could be of any process and not just financial transaction. Given that DLT is suited to assuring consensus, transparency, and integrity of the transactions that it contains, a number of benefits of applying DLT to IdM is as follows[10]:

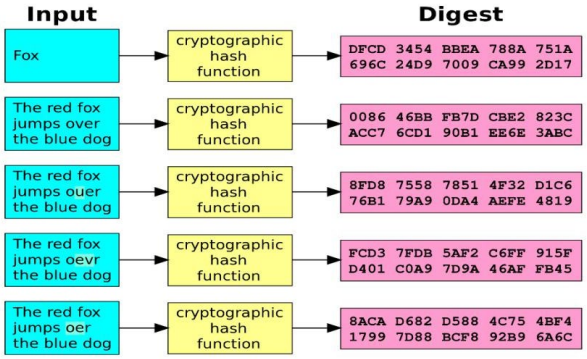
- Decentralised – Identity information is referenced in a ledger that no single central authority owns or control. Tamper-resistant – Historical activities in the DLT cannot be tampered with and transparency is given to all changes to that data.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 07, ISSN No. 2455-2143, Pages 38-45
Published Online November 2023 in IJEAST (http://www.ijeast.com)

- Inclusiveness – New ways to bootstrap user identity can be conceived that expand the reach of legal identities and reduce exclusion.
- Cost saving – Shared identity information can lead to cost savings for relying parties along with the potential to reduce volume of personal information that is replicated in databases.
- User control – Users cannot lose control of their digital identifiers if they lose access to the services of a particular identity provider/broker.

2.1 WORKING OF BLOCKCHAIN

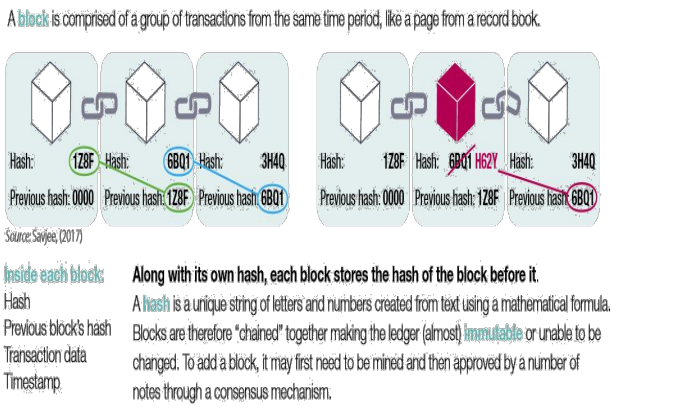
The "pages" on this ledger are blocks where information is stored in a hashed manner, a technique widely employed in cryptography. A mathematical algorithm is applied to convert a piece of information into a string of alphanumeric values, known as the "hash" or "hash value." If the identical information is inputted, it consistently produces the same hash as the output. However, even a minor alteration in the input information will result in a significantly different output hash, a phenomenon referred to as the avalanche effect. Avoiding any correlation between hashes(see fig below).



An example of the hash and how it alters the output with even the slightest change in the letter is given above image. Each block is linked to the next block through a cryptographic hash, and so one, creating a chain. It is a security measure of blockchain technology described below.

2.2 BLOCKCHAIN SECURITY MEASURES

Security measures in blockchain can differ based on specific applications, but commonly include[11]: 1) Employing public-private key encryption for participant access management. 2) Safeguarding transaction data integrity within blocks through cryptographic hashes accompanied by a timestamp. Additionally, the technology systematically documents data blocks by securely linking each block to both preceding and subsequent blocks, as depicted in the figure below.



2.3 PREVENTING FRAUD AND DATA THEFT

Blockchain technology stands out as one of the most effective tools for safeguarding data against hackers, mitigating the risk of fraud, and reducing the likelihood of data theft or compromise. To compromise a blockchain, a hacker would need to erase data stored on every computer across the global network. Considering the vast number of users, potentially in the millions, each with a copy of some or all the data, hacking every node in the network becomes an almost insurmountable task. The hacker would have to compromise a significant portion of the blocks, each containing numerous users' private keys. Consequently, the decentralized nature of blockchain makes a large-scale data breach highly improbable. Larger blockchain networks, with a higher number of users, present an infinitely lower risk of being targeted by hackers due to the formidable complexity required to infiltrate such a network.
This decentralized storage system not only enhances data integrity but also surpasses the availability of centralized databases by design. The intricate structure of blockchain technology positions it as the most secure method for storing and sharing information online that has been discovered thus far. This heightened security has prompted innovators to apply blockchain in various sectors to proactively prevent fraud and enhance data protection.

III. IDENTITY MANAGEMENT WITH BLOCKCHAIN

As explained, Blockchain based identity solutions utilize the concept of asymmetric cryptography for identity management and transaction authentication [12], in order to assign digital identity to things. Several aspects of Blockchain makes the technology suitable for efficient and secure identity management:

1. Blockchain ledger is immutable and transparent (based on permissions), and immutability and transparency are fundamental for identity management.
2. Blockchain is resistant to single point of failure and denial of service attacks.
3. Blockchain provides an efficient implementation of public-key cryptography and hashing, which[13]:

- can be extended for digital identity ownership.

- helps ensuring integrity and authenticity of identity-based records.
- can be utilized for third-party attestation of records.
- helps facilitating permission-based record sharing with smart contracts.

4. Blockchain eliminates or reduces monopoly in identity management, as it is not controlled by a central authority, which also enables identity and record integration in global scale. Blockchain supports incentives via crypto-currencies, which can be utilized for certain tasks such as providing incentives to the participants for data sharing.
5. Blockchain is also considered a system with high Byzantine Fault tolerance. A Byzantine Fault is an occurrence on decentralized systems where it may appear, for one user, that the system is working perfectly and, to others that the system is failing.
6. Blockchains come in two main types: Permissioned and Permissionless.

a. In a Permissionless blockchain, all users have the ability to write on the ledger, and there is no requirement for permission from anyone to become a node on the network.
b. In contrast, Permissioned blockchains necessitate authorization from one or more parties to become a node.

An illustration of a Permissioned Blockchain is Sovrin. In Sovrin, a group of Stewards serves as nodes, and their authorization is vital to maintain the integrity of the information, particularly concerning digital identity recorded on the ledger. These Stewards are individuals or entities trusted and vetted by The Sovrin Foundation.

3.1 ZERO-KNOWLEDGE PROOFS (ZKP)

The name “zero knowledge proofs” is slightly misleading, since the prover A reveals one bit of knowledge to the verifier B. The basic idea is to replace “knowledge” by “knowledge about knowledge”: A’s goal is not to prove that I belongs to L, but to prove that he knows the status of I with respect to L. From B’s point of view, he didn’t get any information whatsoever about “the real world” (I, L and their relationships) - only about A’s state of knowledge concerning the real world[14]. An example in real-world would-be traffic cop checking driver’s information on system where the system returns in a Yes/No manner without showing actual documents. So, its method of authentication with the help of cryptography, allows one entity to prove to another entity that they know a certain information or meet a certain requirement without having to disclose any of the actual information that supports that proof. The entity that verifies the proof has thus “zero knowledge” about the information supporting the proof but is “convinced” of its validity. In an identity management with blockchain scenario, this allows a person to prove that their personal details fulfil certain requirements without revealing the actual details.

Another example is Yao’s Millionaire problem[15] where Alice & Bob without revealing their income, come to know who is richer amongst them. Financial entities use this method, asking in a random way, to their customers about different personal questions that were previously set by them. The problem of authentication arises when user have multiple login situation on mobile phones and other mediums. With the help of ZKP, it uses a RSA to implement, using random number generator for every login instance and the hash (stored in crc32) is added to it and the server counter checks the values for access granting.

A zero-knowledge proof must satisfy three properties[16] -

- Completeness - For a true statement, an honest verifier should be able to be completely convinced the statement is true by a proof provided by an honest prover
- Soundness - For a false statement, a dishonest prover should not be able to convince a verifier that the statement is true.
- Zero-Knowledge - The verifier does not learn anything other than the fact that the statement is true.

3.2 BLOCKCHAIN AS AN IDENTITY MANAGEMENT SOLUTION

Within identity management, a distributed ledger, often referred to as a "blockchain," ensures that all participants on the node share a common source of information regarding the validity of credentials and the attestation of data within these credentials, all without disclosing the actual data. When employing blockchain technology for identity management, it's crucial to recognize the involvement of three distinct actors: identity owners, identity issuers, and identity verifiers.

The identity issuer, typically a trusted entity like a local government, has the authority to issue personal credentials for an identity owner (the user). By issuing a credential, the identity issuer vouches for the accuracy of the personal data contained in that credential, such as the last name and date of birth. The identity owner can then store these credentials in a personal identity wallet and utilize them later to substantiate statements about their identity to a third party, known as the verifier.

A credential comprises multiple identity attributes, and an identity attribute represents a specific piece of information about an individual, such as a name, age, or date of birth.

Credentials are issued by secondary parties who affirm the validity of the information within the credential. The effectiveness and reliability of a credential hinge entirely on the reputation and trustworthiness of the issuer.

3.3 MODELS OF DIGITAL IDENTITY MANAGEMENT

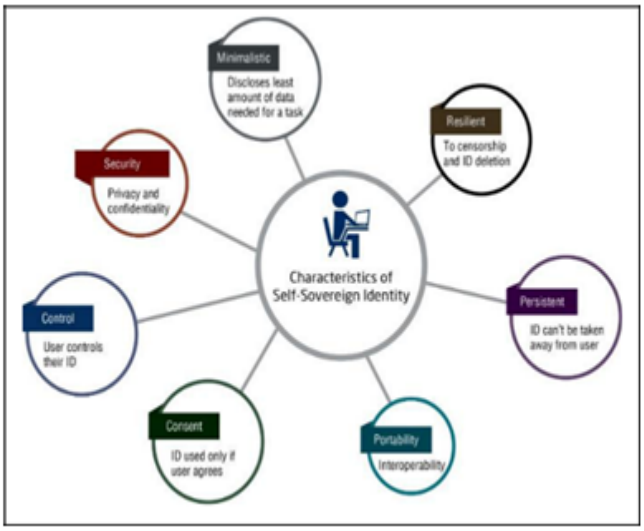
The initial model of digital identity management operated in silos, with each organization providing users with a distinct digital identity credential for accessing its services. Consequently, users had to acquire a new digital identity credential for each new organization they interacted with.

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 07, ISSN No. 2455-2143, Pages 38-45
Published Online November 2023 in IJEAST (http://www.ijeast.com)

Until the last decade, individuals had to register on every website, creating new passwords and login details for each service.
The second model[17], known as "Federated" digital identity management, arose in response to the unsatisfactory user experience of the first model. In this approach, third parties started issuing digital identity credentials, enabling users to log in to various services and websites using a single set of credentials. Examples include functionalities like "Login with Facebook" and "Login with Google." Companies essentially delegated their identity management to major corporations, which, in turn, gathered substantial databases of personal data for economic reasons. However, this outsourcing raised concerns about privacy and security, as platforms like Facebook and Google became intermediaries of trust.

The advent of Blockchain technology paved the way for the third model of identity management: Self-Sovereign Identity.

IV. SELF-SOVEREIGN IDENTITY: WHAT BLOCKCHAIN WILL UNLOCK FOR IDENTITY MANAGEMENT



Self-sovereign identity [18]is a form of identity management where individuals retain absolute control over their personal information. In this system, individuals have the autonomy to decide what information to share, with whom, and for what purpose(see above fig). Utilizing blockchain technology, self-sovereign identity systems offer a decentralized and secure approach to managing identification data, eliminating the need for intermediaries. Lukas et al proposed the complementary considerations for designing systems, which are: 1) Usability, 2) Counterfeit prevention, 3) Identity verification, 4) Identity assurance and 5) Secure transactions.
The idea behind self-sovereign identity is the ability for the identity holders (e.g., users) to have better control over their identity data, with strong emphasis on data portability and data minimization[19]. Lim et al [20] survey provides a critical analysis for existing research which sheds light on various opportunities for enhancing security and privacy of blockchain-based self-sovereign identity management and the improvement of trust management.
Self-sovereign identity (SSI) represents an identity paradigm where individuals, organizations, or entities have complete ownership and control over their own data. This model operates without reliance on centralized authorities, ensuring that the data cannot be arbitrarily removed from the identity owner. The key requirements of an SSI model are outlined table1 below:

Table1: SSI & Key Requirements

Control Over Data	Identity owners have absolute control over the data they possess.
Integrity, Security, and Privacy	The system guarantees the integrity, security, and privacy of the owner's identity without the need for a central authority to establish trust.
Portability of Data	SSI allows full portability of data, enabling identity owners to use their identity data wherever they choose, such as accessing online services.
Transparency	Any alterations to the data are transparent and maintained by the system.

An individual may maintain a single identity across various platforms or may opt for different identities supporting distinct 'personas' for different contexts, such as the workplace, friends, or family. Blockchain technology facilitates this flexibility by providing a unique key for each identity, empowering users to decide which persona to use in specific situations. In essence, self-sovereign identity empowers users to:

- Control Their Identities
- Access and Update Information (though third-party verification may be required for certain claims)
- Choose Private Information

International Journal of Engineering Applied Sciences and Technology, 2023
Vol. 8, Issue 07, ISSN No. 2455-2143, Pages 38-45
Published Online November 2023 in IJEAST (http://www.ijeast.com)

- Transport Data (to another organization or jurisdiction if needed)
- Delete the Identity if des

The ten common guiding principles for an SSI are listed in following table2:

Table 2. Guiding principles for a self-sovereign identity[18].

Principle	Description
Security Dimension	
Protection	The freedom and rights of individual users are the top priority.
Persistence	User identities must persist as long as the user wishes. Even if the underlying data (such as public and private keys) change, the user identity must remain the same.
Minimization	Disclosure of the user data should be minimal, and only the necessary data to verify a claim should be exposed.
Controllability Dimension	
Existence	An identity must be linked to a real person outside the digital world. Thus, users must have an independent existence outside the digital world.
Control	The users should have full control and ultimate authority over their identities and the privacy settings of their identities.
Consent	The sharing of data can only happen when a user provides consent.
Portability Dimension	
Interoperability	Identities should be able to work with any type of system and be available globally without losing user control.
Transparency	The system that operates and manages identities needs to be fully transparent.
Access	A user needs to be able to access all claims and data related to his or her identity.
Portability	Identities cannot be held by a single entity and must be transportable to any other type of system.

Self-sovereign identity (SSI) represents a groundbreaking paradigm shift in identity management, and blockchain technology is the key unlocking its transformative potential. At its core, SSI empowers individuals with unparalleled control over their personal information where an individual, dictate which aspects of his/her identity are shared, with whom, and for what purpose. Blockchain serves as the paradigm of this revolutionary concept, providing a decentralized and tamper-proof ledger that ensures the security and integrity of identity data. With traditional identity systems,

individuals surrender their personal information to centralized authorities, exposing them to vulnerabilities such as data breaches and privacy infringements.

In contrast, SSI on the blockchain enables users to navigate the digital landscape with autonomy and confidence, selectively disclosing information only when necessary. This technology overrides the limitations of conventional identity management, fostering a landscape where trust is distributed, and intermediaries become obsolete. From government services to healthcare, education, banking, and beyond, the impact of SSI on identity management not only mitigates bureaucratic inefficiencies but also addresses global challenges, such as the lack of quality healthcare access and the proliferation of counterfeit academic certificates or where the process could be established to address such lacunae.

By leveraging blockchain technology for identity management, Self-Sovereign Identities may become a reality. A Self-Sovereign Identity is an identity user own & only user hold it, on personal digital identity wallet. And the user allows others to see and its extent avoiding the honeypot problem. As there are no centralised storage of digital identity that may be subject to breaches, for hackers to steal 50 million digital identity records, will require 50 million people individually. Thus, a Self-Sovereign Identity is thus portable, private and secure.

IV.CONCLUSION

A digital identity management system where organisations store the minimum necessary personal data of their users means less personal data management and less bureaucracy reducing data management costs and increasing the efficiency of identification processes. All while putting people's privacy and security first. According to Darrell O'Donnell, a digital identity expert, companies are realising the major liability that is storing personal data of customers (or employees). Every breach, loss or theft of personal data may turn into significant lawsuits and fines. Which may mean that, in the near future, companies will also start working their way into Self-Sovereign Identity solutions. Right now the concern could be of costs and speed but over the time the technology may find its best foot forward.

Identity management with blockchain is benefiting several industries. Reducing governmental bureaucracy, shaping a more efficient healthcare system, detecting academic fraud, creating a better banking experience, helping to provide a more efficient humanitarian aid distribution system and helping companies avoid personal data breaches and GDPR fines. As we walk towaurds the era of self-sovereign identity, powered by the transparency and security of blockchain, we unlock a future where individuals reclaim control over their digital selves, shaping a more secure, efficient, and user-centric landscape for identity management. Right now, this offers a proverbial silver bullet to the present problem of privacy & security but no technology is limitless and absolute.

Future: Self-sovereign identity (SSI), with the help of capabilities of blockchain technology, is on the edge of a futuristic evolution, with Facial Recognition Technology poised to play a important role. The day is not far where your unique facial features become the key to unlocking your self-sovereign identity. In this future landscape, blockchain ensures the secure and decentralized storage of facial data, allowing individuals to control access to their identity with a glance. Its a biometric revolution beyond traditional identity management, offering a seamless and secure authentication process in various sectors. Whether accessing government services, healthcare records, or banking transactions, Facial Recognition Technology integrated with SSI not only enhances security but also expedites processes, avoiding pains of cumbersome passwords and identification documents. This is a futuristic society where individuals, armed with the power of blockchain-based SSI, utilizing facial recognition as a secure gateway to their personal data. As this technology fusion of SSI, blockchain, and Facial Recognition Technology unfolds, it promises a future where identity management is not only secure and efficient but also deeply personalized, marking a paradigm shift to safeguard our digital selves.

V. REFERENCE

[1]. https://www.vmware.com/topics/glossary/content/identity-management
[2]. https://www.nbconsult.co/identity-management/
[3]. Singh, C., Thakkar, R., Warraich, J. ,2023. IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research. 8, Aug. 23, 30–38, https://doi.org/10.24018/ejeng.2023.8.4.3074.
[4]. Devi, Sulochana and Kotian, Shrineeth and Kumavat, Manish and Patel, Dixit, 2022. Digital Identity Management System Using Blockchain. Apr 3, http://dx.doi.org/10.2139/ssrn.4127356
[5]. Applications/Documents/Guides/Digital_Identity_Roadmap_Guide-2018-E.pdf, www.itu.int/en/ITU-D/ICT
[6]. https://auth0.com/blog/how-poor-identity-access-management-equals-security-breaches/
[7]. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
[8]. https://vedveethi.co.in/eNote/BlkChain/HTML_Unit4_New/ Blockchain%20and%20KYC.htm
[9]. Sivasankar G A,2022. Study Of Blockchain Technology, Ai And Digital Networking In Metaverses. International Journal of Engineering Applied Sciences and Technology, 2022 Vol.6, Issue 9, pp 166-169

[10]. Dunphy, Paul; Fabien A. P. Petitcolas ,2018. A First Look at Identity Management Schemes on the Blockchain. Innovation Centre, VASCO Data Security, https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf

[11]. https://www.steptoe.com/a/web/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf

[12]. Howard Poston,2021. Blockchain and asymmetric cryptography, Mar 9, https://resources.infosecinstitute.com/topics/cryptography

[13]. Mehmet Aydara,b, Serkan Ayvazca, 2019. Towards a blockchain based digital identity verification, record attestation and record sharing system. Technology Introduction Department, Huawei Turkey Research and Development Center.

[14]. Uriel Feige, Amos Fiat, Adi Shamir, 1988. Zero-knowledge proofs of identity, Jun '88, Journal of Cryptology, https://arxiv.org/pdf/1906.09791.pdf

[15]. https://encyclopedia.pub/entry/34557

[16]. Saudagar, Pranav; Bhalani, Jayant; Patil, Prasanna; Sharma Shweta; 2017. Zero Knowledge Protocol using RSA Algorithm. International Journal of Engineering Research & Technology, Vol 5, Issue 01, ICIATE – 2017, DOI : 10.17577/IJERTCONV5IS01175

[17]. Shetye Gauri, Nandini Sonar, Dr. Dhanamma Jagli, 2022. Blockchain-based Self-sovereign Identity Management System. International Journal for Research in Applied Science & Engineering Technology, Volume 10 Issue VI Jun '22, //doi.org/10.22214/ijraset.2022.44335

[18]. Stockburger Lukas ; Georgios Kokosioulis , Alivelu Mukkamala, Raghava Rao Mukkamala, Michel Avital, 2021. Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. Blockchain: Research and Applications, Volume 2, Issue 2, Jun 2021, 100014, https://doi.org/10.1016/j.bcra.2021.100014

[19]. Reza Soltani, Uyen Trang Nguyen, Aijun An. 2021. A Survey of Self-Sovereign Identity Ecosystem. Volume 2021, ID 8873429 , https://doi.org/10.1155/2021/8873429

[20]. Lim, S.Y., Musa, O.B., Al-Rimy, B.A.S., Almasri, A. 2022. Trust Models for Blockchain-Based Self-Sovereign Identity Management: A Survey and Research Directions. In: Maleh, Y., Tawalbeh, L., Motahhir, S., Hafid, A.S. (eds) Advances in Blockchain Technology for Cyber Physical Systems. Internet of Things. Springer, Cham. https://doi.org/10.1007/978-3-030-93646-4_13,

International Journal of Engineering Research & Technology, ICIATE - 2017 Conference Proceedings