Transition: Self-Sovereign Identity for Secure Data Management

[1] **Raji Ramakrishnan Nair** , [2] **Ajay Shriram Kushwaha** , [3] **S B Kishore,** [4] **Apash Roy**
[1] Associate Professor, [2] Associate Professor, [3] Research Guide, [4] Associate Professor
[1] Yeldo Mar Baselios College Kothamangalam, rajirknair@gmail.com, [2] School of CS & IT, Jain (Deemed-to-be-University), Bengaluru, kushwaha.ajay22@gmail.com, [3] S P College, Chandrapur s.b.kishor.spc@gmail.com, [4] Lovely Professional University, Phagwara, Punjab, apash.23550@lpu.co.in

Abstract : Data security is said to be the key to privacy. In the era of information technology, data privacy and trustworthy identification has become more important than ever before. In every business, industry even in government organisations, banks, and hospitals launder customer information and use them for their gain. It has a high risk of data breaches. The data is being exploited by them with or without the consent of the individual, who is known to be the actual owner of the data, violating basic human rights and individual privacy. Despite having all the regulations such as GDPR, HIPAA, PDPA, APPI and other available data protection laws, data breaches have become increasingly out of control. With the advancement in technology, it is 'simple' to own and control our own identity. Privacy became a growing concern, because of the various data scandals that occurred in several tech giants recently. This research paper focuses on various solutions available for preventing data breaches to improve data protection and privacy, which can be categorised based on their methodologies that mainly use decentralized technology, blockchain and Open algorithms. Research shows that through the properties of blockchain technology, a solution can be forwarded for adoption by the general public, supported by legal valid status and acceptable performance.

Keywords - Blockchain, Data Breaches, Decentralized Identity, Distributed Ledger Technology, Ethereum, GDPR, Hyperledger, Identity Management, Online Digital Information, OPAL (Open Algorithms), Self-Sovereign Identity, Zero Knowledge Proof.

I. INTRODUCTION

Identity is said to be one of the important parts of any individual. Whatever we do, everything revolves around identity. Earlier the concept of identity seemed to be simple, there was an old paper-based system, but now the situation has changed, where our identities are moving towards digital identity. Making our identity digital is not going to solve all the issues that may come across. There are many factors related to an individual's identity, that must be maintained properly by giving keen importance. Identity is the basic right of any human being. We know that to live in a social environment, we must have an identity. Mainly, any basic identity of an individual consists of Name, Date of Birth and Nationality. Other than all this information, an identity of an individual may consist of a passport number, bank account number, driving license, social security number etc. All these forms of identity-related to an individual vary according to different countries. An individual must have control over their identity otherwise it becomes difficult for an individual even to prove who they say they are. Without proper identification, no one can own property land, use any government services, banking services, voting system or get jobs. Identity plays an important role in any individual's life. Like there are two sides to a coin the data of the people should also be used for the public good to create a better solution for the real-world problems, that is where OPAL (Open Algorithm) can be used. OPAL also aims to reveal the latent of private sector data for public good purposes by *"sending the code to the data"* in a secure, hands-on and bearable manner. Using Open Algorithms, authors try to prevent the movement of data from one party to another and reduce the risk of data breaches.

Digitization of identity became an important factor nowadays because the paper-based old system is proven to be not an apt solution when an individual must prove his or her identity before someone else. Digital identity seems to be a simple concept but it's not actually like that. We know ourselves and we do not need to prove our identity to ourselves. But, when it comes to others, we must show some parameters to others to prove our identity before them. And the parameters that we are using to prove our identity has been generated or supplied by other sources. For example, you are going to travel somewhere on a flight, and you had booked tickets for yourself. When you want to enter the airport, you must have to face the first security check at the entrance of the airport itself. There you must prove your identity before the security officials. The parameters that you are using to prove your identity before they are supplied by some other certified/recognised/authorised sources. The parameters that we are using could be our face, or our name, or any other information related to us. So, in the case of digital identity, any form of distinct information that we use for proving ourselves before others is known as an "identity attribute".

To an individual, different types of identity attributes are connected, such as biometric digital identity attributes like face colour, the shape of the face, gender, voice patterns or fingerprints etc. Other than this, governmental attributes also matter a lot, such as birth date, marital status, current address, etc. As stated in [1], a *"digital identity is a type of identity format where an individual's identity is represented through digital means"*. Digital identity is grouping together various identify attributes.

At present, the digital identity management system is not the best, because it has got major security issues. As the importance of digital identity is increasing it is expected to resolve problems quickly and to ensure a proper management system. Digital identity is important nowadays because of some strong reasons and these are as follows:

- It is difficult to get an education, or access health or banking services without ID.
- Paper-based the old system for identity management is not the best in the present scenario, because of lack of speed and corruption.
- With a paper-based old system for ID, a global connection is almost not possible, whereas digital identity enables that.

Identity management causes serious threats to users while using the centralized database is mostly compromised [2]. According to Cambridge Analytica, a data firm showcase the Facebook scandal which gave unencumbered and illegal access to PII (Personally Identifiable Information) to more than 87 million Facebook users without user permission [3].

Keeping all the issues as the most concerning factor, many identity management solutions came into the picture. Research showed that a solution built on blockchain technology is a good foundation to solve all the major issues of identity management systems [4]. In this paper, the authors focused on almost all the solutions to identity management built on blockchain technology. Authors also stated that they are working to provide alternatives and over weaknesses of current identity management systems built on blockchain technology to apply decentralized identity (DID) and self-sovereign identity together to come up with solutions to overcome all the weaknesses that existing identity management systems possess.

II. LITERATURE REVIEW

A typical digital identity management system has come across with serious issues. Some of them are listed below [1]:

a) Bad Personal Combination

Most of the today's applications force us to enter into it using only password-based login authentication system, which remains valid for only a stipulated period. Because of this reason, we must face the problem of "password fatigue" and we start to use the same password for multiple applications increases the security risk for identities.

b) Ineffective security measures utilization

Today's digital identity management system lacks an instant alert system to keep track of all the users. It also lacks proper security channels and the storage system is not immutable, which enables anyone to abuse other people's identities. This improper management of digital identity leads to identity theft and cybercriminals.

c) Repetitive registration or KYC process.

Same repetitive registration or KYC processes is important issues of digital identity system. As we have multiple platforms for multiple applications, we must register for each platform separately, which is repetitive process, leads to wastage of time as well as data and privacy breaches. For example, if we want to open a bank account at State Bank of India, we must fill one KYC form. And, suppose we want to open another bank account at ICICI Prudential Bank, then again, we must fill another KYC form, so repeating the same process what we did earlier.

d) Centralized servers issuing identities.

In traditional method, identities are issued by centralized servers only. The major issue that persists here is that many citizens even do not have proper identity.

e) Companies can easily mishandle personal information.

As we all live in the digital world, every company tries to exploit us by using our data for their selfish reasons. Such data and privacy breaches have been identified in the recent past with popular tech giants. There should be strict protocols ensuring data privacy and security.

Decentralized identity is a lot of things to a lot of people. As a human being, we can identify ourselves without worrying about theft or fraud. Distributed Ledger Technology (DLT) has revolutionized the digital identity by taking away the power of proprietorship of private data of any individual from multinational marketing companies and governments to the individual itself [5]. DLT is to be appropriate to safeguard transparency, consensus and integrity of all the transactions that it contains, also it has got several benefits such as decentralization, tamper resistant, inclusive, cost effective and user control [6]. Whereas Self-Sovereign Identity (SSI) is one of the available concepts where people and businesses store and control their data on their devices, further data will be provided to someone who needs to validate collected data which removes the centralized database concept. Those who work on or with identity systems, need to obey the "*Laws of Identity*". Otherwise, lead to supplement side effects that could sabotage all resulting technology. By following these laws, will help us to build a unifying identity metasystem that is universally accepted and enduring [7]. Examples of frameworks using SSI are Sovrin, uPort, OneName and examples of frameworks using decentralized identity are ShoCard, BitID, ID.me, IDchainZ.

Zyskind et al. stated the concept of "*blockchain as vessels for identity*". Whereas C. Allen said, "*the path to self-Sovereign identity its definitions and requirements for User-Centric and Self-Sovereign Identity is formed based on Dutch government stance and policy on self-governance identity*". According to study world's first *permissioned decentralized* digitized passport and a true peer-to-peer common identity has been explained and presented by Netherlands for use and practice by their citizens after mid of 2018 as a solution to self-sovereign identity [8] [9] [10] [11].

Self-Sovereign Identity solutions can be created using blockchain or without implementing blockchain. In [4], it has been found that solutions implemented using blockchain satisfies almost all the properties listed by K. Cameron and C. Allen. The solutions which uses blockchain are uPort [12], IDchainZ, EverID [13], Sovrin [14], LifeID [15], SelfKey [16], Shocard [17], Sora [18]. Out of these, LifeID, SelfKey, Shocard, and Sora follows all the eleven properties listed by K. Cameron and C. Allen. Those solutions which are not implemented using blockchain are PDS (Personal Data Store), IRMA (I Reveal My Attribute) [20] and reclaimID [19]. The comparison [4] highlights how on average blockchain-based solutions is capable to meet more properties which was not possible without using blockchain technology.

"Dragon Factor is another decentralized identify solution based on blockchain technology" which gives importance to privacy and control of user's data. To design Dragon Factor, privacy principles has been used from GDPR - compliant blockchain solution which does not expose any personal identifiable information [21].

Whereas in traditional approach used by large banks and other security firms use to access and employ personal information of customers to give enhanced experience [22]. We have given them a "Green Signal" so that they can use our sensitive details the way they want. Then came the blockchain technology and changed the whole situation drastically. But time has proven that with blockchain network, our sensitive data is only confidential, not anonymous. There are many methods like Coin Mixing, Ringct and Coin join, which helps transactions in blockchain to be anonymous, but the one which is highly appreciated is "*Zero Knowledge Proof (ZKP)".*

"Zero Knowledge Proof" is another type of Self-Sovereign identity and identify management solutions built on blockchain. ZKP system works to prove a verifier is true or not without revealing any other additional information which solves the purpose of identify security. Currently highly anonymous cryptocurrency *Zcash* ensures anonymous transactions with *"Zero Knowledge Proof"*. For example, A wants to prove to B that he possesses the key to a certain room, and the room can only be unlocked with the key. Now, A can choose to hand the keys over to B and B uses the key to unlock the room, proving that A holds the correct key. Alternatively, A himself can unlock the room using the key and showing an item to B, who know that it is only available in that room. The principle behind the latter method is Zero Knowledge Proof. ZKP is proving that one knows the password without conveying any other information. This effectively solves many verification related problems. ZKP has a wide scope for research. It has two variants: Interactive ZKP and Non-Interactive ZKP [23].

Further important concern is to ensure security and preserving privacy of all identities stored in big giant's databases. They are using all those details for their individual research and development purposes. OPAL (Open Algorithms) in partnership with MIT lab is non-profitable socio-technological innovation project which is focused on how to manage multiple identity details for better decisions. The data sets with tech giants or industries or government, if fine-tuned well, have the power to shed light on various socio-economic issues of a country such as crime, diseases, poverty, inequality, urban congestion and many more to maintain all such data sets positively [24].

III. CONFUSION

This paper states that identity management solutions can be solved using blockchain as well as using non-blockchain technology. It is also found that on average blockchain based identity management solutions are adhering almost all the properties of the Law of Identity. Since blockchain technology has privacy and security issues, that means identity stored in blockchain is confidential, but it is not anonymous. So, the concept of *Zero Knowledge Proof (ZKP)* is used to verify that statement argument as true without skimpy any additional information to verifier. Open Algorithms are identity management solution, which is not using the blockchain technology for better decisions. Further authors urge attention of researchers to explore this area to strengthen the weakness of self-sovereign identity transition to self-sovereign data management in effective way.

REFERENCES

[1] "ccf17dcfefa1ae5ed8942ca27ec609f1cd0ad8b9 @ 101blockchains.com."

[2] S. Y. Lim et al., "Blockchain technology the identity management and authentication service disruptor: A survey," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 4–2, pp. 1735–1745, 2018.

[3] J. Isaak and M. J. Hanna, "User data privacy: Facebook, Cambridge Analytica, and privacy protection," Computer, vol. 51, no. 08, pp. 56-59, Aug. 2018.

[4] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology," pp. 1–8, 2019.

[5] Richard Chen, "Understanding Decentralized Identity - A Missing Piece of Infrastructure for the dApp Ecosystem", an article published by medium.com on dated 7th September 2018, URL- https://thecontrol.co/understanding-decentralized-identity-433abb343279 (Retrieved - 03/03/2020).

[6] Paul Dunphy, Fabien A.P. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," pp. 20 – 21, 2018.

[7] Kim Cameron, "The Laws of Identity," 2005.

[8] Guy Zyskind, Oz Nathan, et al., "Decentralizing privacy: Using blockchain to protect personal data," In Security and Privacy Workshops (SPW), 2015 IEEE, pages 180-184. IEEE, 2015.

[9] Christopher Allen, "The path to self-sovereign Identity, an article published by www.lifewithalacrity.com on dated 25th April 2016, URL- http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (Retrieved – 03-03-2020)

[10] Marvin van Wingerde, "Blockchain-enabled self-sovereign identity," Master's thesis. Tilburg University. School of Economics and Management, 2017.

[11] Quinten Stokkink, Johan Pouwelse, “Deployment of a Blockchain-Based Self-Sovereign Identity,”. In IEEE Confs on IoT, Green Computing and Communication, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, 2018 IEEE.

[12] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, “uPort: A platform for self-sovereign identity,” by uPort a techreport published on 20th October 2016, PDF URL - http://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf (Retrieved - 03-03-2020)

[13] B. Reid and B. Witteman, “Everid whitepaper,” published by EverID techreport, published on July 2018, PDF URL - https://icorating.com/upload/whitepaper/KK6mLeOuHR85wy3pvpO6rhxqUx6BRSC8bR6PXMMS.pdf (Retrieved - 03-03-2020)

[14] R Joosten, “A conceptual analysis on Sovrin,” as on January 2018.

[15] LifeID, “An open-source, blockchain-based platform for self-sovereign identity,” published by LifeID a techreport, published in 2018, PDF URL - https://lifeid.io/whitepaper.pdf (Retrieved - 03-03-2020)

[16] SelfKey, “SelfKey” by The SelfKey Foundation, a techreport, published on 11th September 2017, PDF URL - https://selfkey.org/wp-content/uploads/2019/03/selfkey-whitepaper-en.pdf (Retrieved - 03-03-2020).

[17] Armin Ebrahimi, “Identity Management verified using the Blockchain,” published by ShoCard a whitepaper techreport in 2019 PDF URL - https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf (Retrieved - 03-03-2020)

[18] M. Takemiya and B. Vanieiev, “Sora identity: Secure, digital identity on the blockchain,” in 2018 IEEE 42nd Annual computer Software and Applications Conference (COMPSAC). IEEE, Jul. 2018.

[19] M. Schanzenbach, G. Bramm, and J. Schutte, “reclaimID: Secure, self-sovereign identities using name systems and attribute-based encryption,” in 2018 17th IEEE International Conference On Trust, Security And Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science And Engineering (TrustCom/Big – DataSE). IEEE, Aug. 2018.

[20] Jelle C. Nauta, Rieks Joosten, “Self-Sovereign Identity: A Comparison of IRMA and Sovrin”, a techreport published under project Techruption on dated 14th July 2019, PDF URL - http://publications.tno.nl/publication/34634504/uwmOQq/TNO-2019-R11011.pdf (Retrieved - 03-03-2020)

[21] Dragonchain, “5 Things You Should Know About Dragon Factor”, an article published by dragonchain.com on dated 21st August 2019, URL - https://dragonchain.com/blog/5-things-you-should-know-about-dragon-factor/

[22] Chirag Bhardwaj, “What is Zero-Knowledge Proof & its Role in the Blockchain World?”, an article published by appinventiv.com on dated 9th January 2020, URL - https://appinventiv.com/blog/zero-knowledge-proof-blockchain/

[23] D. Cerezo Sánchez, “Zero-Knowledge Proof-of-Identity: Sybil-Resistant, Anonymous Authentication on Permissionless Blockchains and Incentive Compatible, Strictly Dominant Cryptocurrencies,” *SSRN Electron. J.*, 2019.

[24] Thomas Hardjono, Alex Pentland, “Open Algorithms for Identity Federation,” Conference paper. Springer, December 2018.