Comparative Study of Blockchain based Verifiable Credentials

Prof Riyaz Jamadar[1], Gaurav Bade[2], Hetal Parmar[3], Krishna Waske[4]

Dept. of Information Technology, AISSMS's Institute of Information Technology Pune-1, Maharashtra, India

---

Abstract - *Identity is a fundamental right of every human being. Identity Provides a sense of belonging over the diverse nature of surroundings. It has a major role to play in a fast-paced world of digitization where the prime tagging of entities is done over their physical identities. "On the Internet, nobody knows you're a dog" is an adage about Internet anonymity that began as a caption to a cartoon is drawn by the Peter Steiner, and published by The New Yorker on July 5, 1993. And with rapid growth and developments over the past decades in consumer internet, the situation still holds true. The identity layer over the internet still seems to be broken and mismanaged. The paper is intended to shed light on the possibility of introducing this missing identity layer on the internet by proposing a blockchain-based identity that is sovereign to the holder. The solution can promise complete control or possession over the generation, distribution, and storage of identity. All this while eliminating the need for a central authority to store and manage identity on behalf of an individual, eliminating implied trust over the central authority*.

Key Words: Self-Sovereign Identity, Credentials, Blockchain.

1. INTRODUCTION

Credentials are an integral part of one's identity and hence play a vital role into providing value at most stages. Also preserving the integrity of any document is also a vital part of verification. The paper focus of comparing various literature paper available and the approach individually implemented or suggested by the respective authors of the publications. The domain of SSI mainly focuses on maintaining the integrity of credentials issued by the issuer and also provides a tamper less and verifiable solution. The verifying organizations can easily verify whether changes are made to the document by the holder (of the credential). This can help delegate or transfer trust from the holder to the issuer itself. All the integrity part is handled by the underlying self-sovereign system.

2. LITERATURE SURVEY

[1] Revocable and Offline-Verifiable Self-Sovereign Identities:

To show the concept's, an implementation has been developed and evaluated that includes an efficient and privacy-preserving showing of credentials using non-interactive zero-knowledge proofs, all while being offline. Supporting both revocation as well as verification in an offline setting remains a challenge. In contrast to the paper-based world, it is not feasible to take back and destroy digital information. This work proposes a general concept enabling offline authentication of revocable SSIs serving as a basis for future real-world implementations. It is an advanced research focusing on wider adaptability and robust usage.

[2] Self-Sovereign Identity Specifications:

It Governs our Identity Through our Digital Wallet using Blockchain Technology. The paper proposes several specifications to be evaluated by any SSI solution. Subsequently, it analyzes two emerging SSI solutions uPort and Sovrin. This comparison is basis of multiple points being considered to differentiate the solution The paper focuses on studying and analyzing SSI solutions rather than providing a base knowledge of implementation and other aspects. The paper also proposed specifications for evaluating emerging SSI solutions. Subsequently, it analyzed two emerging SSI solutions uPort and Sovrin including their architecture, components and working.

[3] In Search of a Self-Sovereign Identity Leveraging Blockchain Technology:

The main methodology used is a comparative study and focuses on comparing the available SSI solutions. It also provides an in-depth overview and a decent mathematical and algorithmic insights. They have highlighted the subtle difference between an ideal identity system and an SSI system in the article. In addition, they have created mathematical notion of property to classify them accordingly. This paper presents the first formal and rigorous treatment of the concept using a mathematical model. It highlights the life-cycles of an identity management system and inter-relates how the notion of self- sovereign can be applied.

[4] A Comparative Survey on Blockchain-based Self-Sovereign Identity System:

The paper presents existing implementations of identity management on the blockchain with a focus on properties of self-sovereign identity and discusses their

characteristics. The paper envisions that there may be numerous potential use cases for Self-sovereign identity that provides users the capability to govern their identity credentials In this paper, they have discussed fundamental principles related to SSI along with its architectural components. They have further analyzed and compared various blockchain-based SSI models.

3. DISCUSSION

Self-Sovereign Identity (SSI), according to the authors of paper [1], is a manifestation of a user-centric digital identity management model. SSI puts the control over the identity data in the hand of the data subject, by issuing and handing over a credential that contains certified attributes. This credential needs to be digitally signed by a qualified authority in order to protect the integrity and authenticity of data. The SSI network's distributed ledger allows nodes to issue attestations about the revocation status of a credential, which they sign using multi-signatures. Their concept builds a bridge between systems that rely on queries to a revocation database and systems that require short-lived credentials. The paper [2] specifies, identity as one of the biggest problems in the digital era. Since its inception, several Identity Management (IDM) models have been created and implemented in this field, but only a select handful have been successful in addressing the problems of an identity's sovereignty and the storage-control of the associated personal and private data. Self-Sovereign Identification (SSI), which provides users with total control over their identification and the preservation of their related private and sensitive data, was created to address this critical issue. It stores all personal information in a digital wallet that the user owns and controls in addition to retaining identity ownership. However, because SSI is a new IDM, its numerous components must be thoroughly investigated before it can be utilized as an IDM.

The concept of self-sovereign identity is an exciting prospect. It has the potential to liberate any user, for the first time ever, from the parochial control of an organization regarding the management of her identities. Unfortunately, existing works are not methodological and they do not explore the topic in a more formal way. This article[3] contended against the notion and argued that many of these properties belong to an identity management system. Self-sovereign identity management systems could be realized in a smart-contract supported blockchain system.

Identity management is a very important domain to access services from different service providers. In current scenario, it is very difficult for service providers to manage large number of users and at the same time users do not have any control over their identity information. There is a need to change trust management in digital identity from centralized to decentralized environment. This paper[4] supports the literature by contrasting actually available blockchain-based self-sovereign identity models.

4. CONCLUSION

Modern daily life is largely reliant on digital identification. Online interactions are made easier and more secure thanks to ongoing technical advancements in this field. Providing a digital form of identification that replicates actual paper-based identities and transactions is the foundation of digital identity. Digital identification is essential for enterprises. For companies to remain competitive against those that have embraced developing technology earlier, it is crucial to offer ways for users to connect with digital services safely and securely. A crucial element is privacy. Businesses need to have confidence in the security of their systems and the protection of their personnel and customer data from both insider and outside threats. Customers and employees must also feel in control of and secure with their data.

REFERENCES

[1] Abraham, A., More, S., Rabensteiner, C., & Horandner, F. (2020). Revocable and Offline-Verifiable Self-Sovereign Identities. 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). doi:10.1109/trustcom50675.2020.

[2] Nitin Naik and Paul Jenkins. Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology, 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud).

[3] Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access, 1–1. doi:10.1109/access.2019.2931173 .

[4] Jayana Kaneriya and Hiren Patel, A Comparative Survey On Blockchain Based Self Sovereign Identity System, 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) DOI: 10.1109/ICISS49785.2020.9315899

[5] Quinten Stokkink and Johan Pouwelse, Deployment of a Blockchain-Based Self-Sovereign Identity, 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, DOI 10.1109/Cybermatics_2018.2018.00230

BIOGRAPHIES

Mr. Riyaz Jamadar
Assistant Professor
Department of Information Technology
AISSMS IOIT , PUNE

Gaurav Bade
BE -IT
AISSMS IOIT ,Pune

Hetal Parmar
BE -IT
AISSMS IOIT , Pune

Krishna Waske
BE- IT
AISSMS IOIT , Pune