ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

Blockchain Solutions for Identity Management

Arundhati Mishra [1], Menita Agarwal [2], Varun Chandra Gupta [3], Dr. Seema Shah[4]

U.G. Student, Department of Computer Science, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India [1]

U.G. Student, Department of Computer Science, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India [2]

U.G. Student, Department of Computer Science, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India [3]

Professor, Department of Computer Science, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India [4]

ABSTRACT: Managing identity online has become increasingly common these days. With personal records of millions of people online, security and privacy are vital. Frequency of data breaches in the past few years has raised concerns about security capabilities of current digital Identity Management Systems. The Blockchain technology is gaining traction in the world and amongst its wide range of applications, authentication systems are emerging. In this paper, the issues surrounding the present digital identity management schemes and how Blockchain can resolve them is discussed. The paper looks at Self Sovereign Identity solutions and examines the most popular Identity Management Systems that use Blockchain: uPort, Sovrin, and ShoCard.

KEYWORDS: Digital Identity, Identity Management systems, Blockchain, Privacy, Distributed Ledger

I. INTRODUCTION

Today Digital identity is paramount for a lot of services. Services like authentication, authorization, secure exchanges and transactions are built on digital identities. The concept of a digital identity is being pursued around the world and governments aim to digitize their citizens.Digital Identity Management Systems (IdMS) are responsible for managing users' information, consisting of identifiers and credentials like Email IDs, username, password, biometrics, etc. IdMS manages identity details through a set of operations like registration, administration, updation, and maintenance of identities.With digital identity becoming of great importance, the question of how secure current identity management schemes are surfaces. The frequency of hacks in the past years has highlighted this issue and the associated challenge of protecting the digital data of users. This emphasizes the need for a storage system technology that is robust to system failure and security attacks, secure and reliable. One of the promising solutions for this is Blockchain. Blockchain is a distributed ledger which records transactions between two parties efficiently and in a verifiable and permanent way[1].
The structure of the paper is as follows: Section III talks about the challenges faced by digital identity methods. Section IV includes the role of Blockchain Technology and how its features are beneficial in Identity Management. Section V introduces the emerging concept of Self-sovereign identities and discusses the current Blockchain based IdMS. The VIth Section draws a conclusion and presents future directions.

II. RELATED WORK

In 'A First Look at Identity Management Schemes on the Blockchain' [2] by Paul Dunphy and Fabien A.P. Petitcolas,three DLT(Distributed Ledger Technology) Sovrin, uPort and ShoCard are evaluated and compared with respect to the seven laws of identity stated by K. Cameron.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

In 'Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology' [3] the Self-Sovereign Identity solutions are inspected and their implementations under multiple aspects are dissected to understand if blockchain is a necessity or not. It is concluded that blockchain is not a necessity but a good foundation for SSI.
In the White Paper 'The Inevitable Rise of Self-Sovereign Identity' by Sovrin Foundation [4], Christopher Allen's Ten Principles of Self-Sovereign Identity is grouped into three sections: security, controllability and portability. Self-Sovereign Identity is referred to an identity which satisfies criteria relating to these sections.

III. DIGITAL IDENTITY CHALLENGES

With critical records and data of millions of people digitized, security and management are the primary concerns. Data breaches are not uncommon these days, hence privacy and protection of data has become one of the biggest challenges. Especially for companies and institutions who have large user databases and tons of personal records regarding their clients stored on their servers which are centralised. Most user authentication methods and identity verification systems rely on such a centralized database where all information needed to authenticate an individual is kept in one place. Such information storage presents a single point of compromise from a security perspective [6]. If this system is compromised it poses a direct threat to users' digital identities. For a digital ID system to work without becoming an easy target for hacking, it should be decentralized. Moreover, users have to put all trust on third-party identity providers. These identity providers could see all the exchanges between users, which undermines their privacy.The investigation of alternative approaches to IdM is ongoing. One of the proposed methods for this is Blockchain. Blockchain is emerging due to its decentralized architecture and distributed public ledger technology.

IV. BLOCKCHAIN IN IDENTITY MANAGEMENT

Blockchain is a technology that holds enormous potential to protect our records from data manipulation and ensure their longevity. The core of a blockchain network is a distributed ledger that records all the transactions that take place on the network. The following attributes of Blockchain explain why Blockchain has huge scope to become a new system of trust:

- **a) Decentralized:** Identity information is stored by a ledger that no single central authority owns or controls. There is no single point of failure since data is distributed. Data is recorded in different places, making it less prone to system attacks and failure.
- **b) Confidentiality and Privacy:** To access any service, users use their digital identity to authenticate and authorize themselves. Traditionally, these digital identities are offered by a central identity provider belonging to a specific organisation [8]. Identity providers could retain information about service accessors and service owners and could trace all transactions between them. Users have to take this risk and put their trust on third parties.
- **c) Persistency:** Transactions can be validated quickly. It is impossible to rollback or delete transactions once they have been included in the blockchain. Blocks that contain invalid transactions could be discovered immediately [9].
- **d) Tamper free:** Blockchain provides security by being immutable. The structure of Blockchain makes it impossible to make adjustments to the data after they have been recorded in a distributed database. In addition, the information recorded to a blockchain is append-only, using cryptographic techniques that guarantee that once a transaction has been added to the ledger, it cannot be modified[10]. This property of immutability makes it simple to assure that data has not been tampered. If any updates have to be made, they are validated against strict criteria and added to the blockchain only after a consensus has been reached. Additionally, timestamping is used which could be used for building trust relationships.

V. IDENTITY MANAGEMENT BASED ON BLOCKCHAIN

People don't have control over how their data is protected or used, which is a huge concern. The emergence of Self-sovereign identity can change this. Self-Sovereign Identities recognizes that an individual should own and control their

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

identity without the intervening administrative authorities [11]. SSI is a model for managing digital identities in a way where an individual has sole ownership over the ability to control their accounts and personal data. There is no intermediary involved, providing users with the privacy they should have over their information. Individuals with self-sovereign identity can store their data to their devices and provide it for verification and transactions whenever needed without the need to rely upon a central repository of data [12]. With self-sovereign identity, users have complete control over how their personal information is kept and used and they decide when and with whom their information is shared. Considering everything, the best way to implement a system with self-sovereign identity would be through Blockchain technology as it eliminates the need for any intermediaries or third-parties.

1. uPort:

uPort is a Self-Sovereign Identity system based on Ethereum smart contracts. It is open source and decentralized. uPort allows users to register their own identity, send and request credentials, digitally sign transactions, and securely manage keys & data.

a) Design:

The uPort technology consists of three main components: smart contracts, developer libraries, and a mobile app. Fig.1 shows these three components and what each component comprises of.

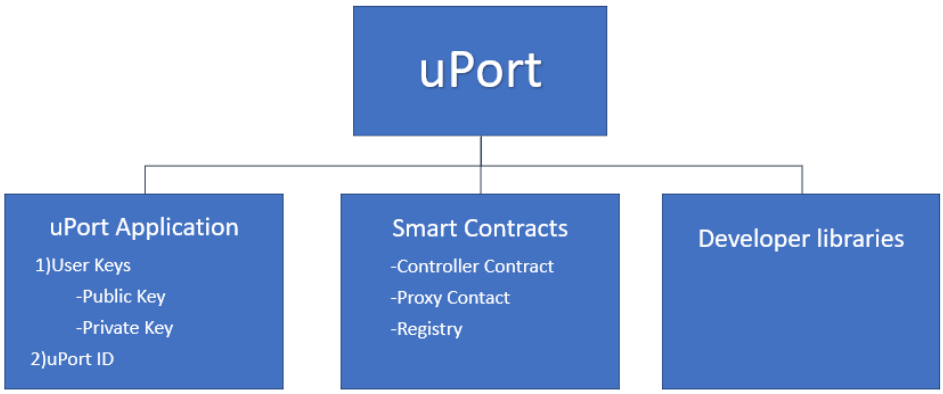

Fig. 1: Three maincomponents of uPort: uPort mobile application, smart contracts and developer libraries.

To create a new identity, an asymmetric key pair is generated by the uPort application. uPort has two main smart contract templates: controller contract and proxy contract. Generation of keys lead to the creation of a new controller that stores a reference to the public key. Then, a new proxy is created that contains a reference to the just-created controller contract [2]. The proxy can only be accessed by the controller. When the user wants to interact with a particular application smart contract, they send a transaction through the Proxy contract, via a Controller contract, which contains the main access control logic. The Proxy contract then forwards this transaction to the application smart contract [13].

Hence, proxy contract is the entity that interacts with the application. At the core of a uPort identity is the uPort identifier, a 20-byte hexadecimal string that is a globally unique identifier. This identifier is defined as the address of proxy contract. The private key associated with a uPortID is stored only on the user's mobile device. As a result, losing the device would mean losing the key. For this, uPort has an important feature of key recovery protocol where users must nominate trustees, who can vote to set a new public key for the user via the controller. A quorum has to be reached and then the key is replaced. Another component of uPort is the registry contract which maintains a mapping from a uPortID to identity attributes. However, to reduce storage volume, only the hash of the JSON attribute structure is stored in the registry. The data itself is stored on IPFS, a distributed file system where data can be retrieved by using its cryptographic hash. Fig. 2 gives an overview ofuPort's structure and how it works.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

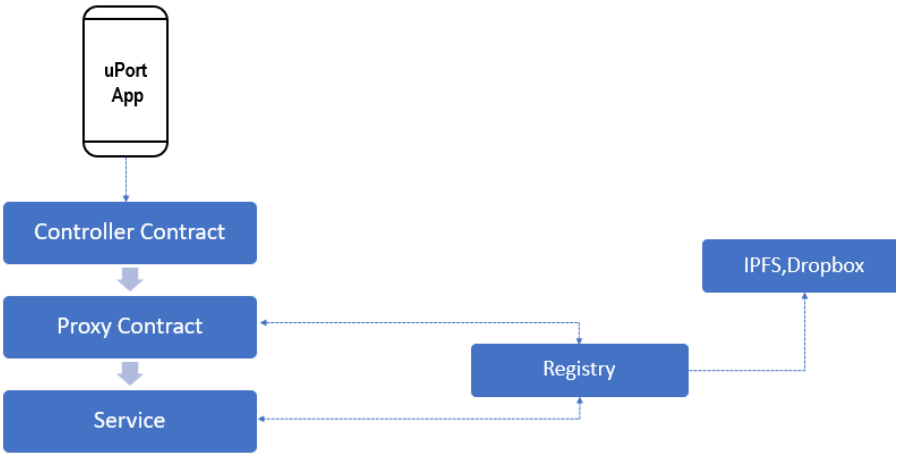

Fig. 2:Architecture of the interaction between uPortID and the smart contract of a service on Ethereum.

b) Analysis:

- uPort provides a platform where users can create uPortIDs without involvement of a central authority.
- Information is collected only on a "need-to know" basis, hence users don't need to disclose personal information for a constrained use.
- uPort respects privacy in terms of the lack of inherent likability between uPortIDs [2]
- Integrity of data is guaranteed as only the owner of a specific uPortID can modify its respective attributes.
- Discreet disclosure of a uPortID is possible if the user creates new uPortIDs for each new party.
- The key recovery feature enables the user to maintain the same uPortID even after the loss of cryptographic keys.
- uPort has no user authentication method for users, creating the possibility of unauthorized access
- The trustees appointed for key recovery could be a point of attack or harm
- The registry acts like a centralised datastore, which could be probed for information. Even when the identity attributes are encrypted, the JSON structure is visible, through which metadata about attributes could be leaked.

2. Sovrin:

Distributed ledgers are of two types—public and private. Sovrin is a hybrid between these two models— a public permissioned ledger, providing public access and trust with high throughput. Sovrin can be used by anyone but only trusted and known set of validator nodes, called stewards can take part in consensus mechanisms.

a) Design:

Sovrin has been designed to satisfy the four major requirements of SSI: governance, scalability, accessibility, and privacy [14]. Sovrin lets a user create as many identifiers as they need, and these identifiers are decentralized. Decentralized Identifiers (DID) are a type of identifier designed for cryptographically-verifiable digital identity that is independent or self-sovereign [15]. A DID contains the user identifier, cryptographic public key, and other metadata necessary to initiate trusted peer interactions between Sovrin entities.

The architecture consists of three layers, as shown in Fig. 3:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

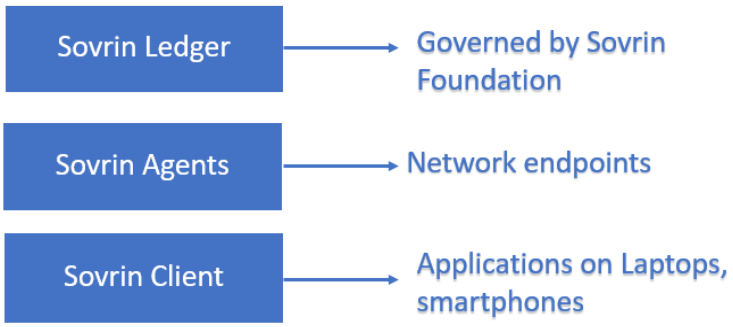

Fig. 3: Architecture of Sovrin consisting of Sovrin ledger, Sovrin agents and Sovrin clients.

(i) Sovrin Ledger: It is the key component of Sovrin architecture. It is a globally distributed ledger containing root identity records and is maintained by trusted institutions, stewards, around the world. Stewards nodes run the Plenum protocol, an enhancement version of the redundant Byzantine fault tolerant protocol [7], to achieve consensus. Sovrin Foundation is a global non-profit organisation whose sole purpose is governance of this ledger. It contains identity transactions associated to a particular identifier and is written, distributed, and replicated among the steward nodes, which run an enhanced version of the redundant Byzantine fault-tolerant protocol of Aublin and colleagues, called Plenum, for consensus. is the foundational component—a globally distributed ledger of root identity records maintained by trusted institutions around the world. The structure and operation of this layer, operated as a non-profit global public utility governed by the Sovrin Foundation.
(ii) Sovrin Agents: They are a new type of network service that give Sovrin identity owners (people and organizations) a permanent, privacy-protecting way to perform identity and data management transactions [5]. Users interact with Sovrin though agents. They are the middle layer in the architecture. Agents are network endpoints that make Sovrin clients addressable.
(iii) Sovrin Clients: Applications used by Sovrin Identity owners to communicate with Sovrin agents and the ledger for identity transactions. They are the final layer of the Sovrin architecture and are vital. The single most critical function of a Sovrin client is to manage and protect the identity owner's Sovrin cryptographic keys.

b) Analysis:

- Sovrin architecture implements the unique combination of a public DLT operated by permissioned nodes that are governed by a global non-profit foundation.
- No mining or expensive proof-of-work is required since the ledger is permissioned, hence the system does not need immense computing power and can run at a much higher throughput than permissionless blockchains.
- Sovrin equips users with a full control of their identity. They can choose the attributes they wish to share with relying parties. The verification of these latter remains a challenge, which is partly addressed through the web-of-trust, the governance of the Sovrin Foundation and the reputation of the stewards [2].
- Sovrin eliminates need for third parties, users interact with Sovrin through applications (Sovrin agents).
- Ledger is operated by a global network of trusted institutions, all of whom are monitoring each.
- Sovrin supports minimal disclosure of identity information. Users can choose which identifiers they want to disclose. Only the attributes necessary for that particular transaction are revealed.
- Support is provided for sharing identity information publicly or in a discreet way. Public organizations can decide to publish their full identity on the network, while users may choose to reveal only necessary identifiers and to use different identifiers and cryptographic keys with each party they interact with.
- A mechanism for key recovery exists, that relies on the user selecting a set of trustees. A quorum must be reached and verified by stewards.
- There is no centralized storage, identity records live redundantly across all Steward nodes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

- Although, there are no third parties, users must rely on the stewards maintaining the distributed ledger.
- Sovrin is not deployed widely due to users finding the interface too difficult to understand. Human integration and consistent user experience remain a challenge for Sovrin.

3. ShoCard:

ShoCard is a mobile digital identity platform that integrates Blockchain, identity attributes and biometrics for managing identity digitally. The architecture relies on Bitcoin Blockchain. ShoCard binds a user identifier and an existing government issued identity credential, like passport or driver's license, together via cryptographic hashes and is stored in Bitcoin.

a) Design:

The scheme is based on three phases:

(i) Bootstrapping: It takes place at the creation of a new ShoCard. The ShoCard application generates a new asymmetric key pair for the user and scans their identity credentials using the device's camera. The scanned credentials and data corresponding to them is encrypted and stored on the mobile device. The signed hash of this data is stored on Bitcoin too as ShoCard seal and the resultant Bitcoin transaction number constitutes the user's ShoCardID.

(ii) Certification: After the bootstrapping phase, the user has to confirm their identity by interacting with an Identity Provider. The user sends their encrypted credentials to the Identity Provider which verifies them against the user's entry on the Blockchain. When the records sent by user and the records stored on the Blockchain match, the certificate is associated with the user's ShoCardID by the provider. The certificate is stored as signed hash in the Bitcoin transaction created by the provided. Encrypted certifications associated with a ShoCardID are stored on ShoCard server and are known as envelopes.

(iii) Validation: The validation phase occurs when a relying party must verify a certification to determine whether a user is entitled to access a service. User provides the relying party with the envelope reference and its encryption key. The envelope itself is provided by the ShoCard server.

The relying party validates the received envelope for:

- whether the envelope signature and signed ShoCard seal was generated by the same private key
- the envelope signature was created by a trusted organization.

b) Analysis:

- ShoCard never stores the encryption key for user's data envelope, hence users control the disclosure of their identity with the relying parties entirely.
- ShoCard uses Bitcoin as a timestamping service for storing signed cryptographic hashes of the user's identity information in the Bitcoin blockchain.
- The bootstrapping phase requires binding of an existing user credential with identity attributes. This does not support minimum disclosure, since more than just needed information has to be provided by the users
- The ShoCard server acts as an intermediary in the distribution of encrypted certificates between the user and relying party. If the company ceased to exist, users won't be able to use the system with certificates issued to them. This makes ShoCard server centralized and an entity user have to be dependent on.
- ShoCard server may be able to associate a particular ShoCardID with a particular relying party.
- There is no public registry that maintains ShoCardIDs. It only supports unidirectional identifiers.
- User interaction is simple and consistent.

VI. CONCLUSION

The deficiencies of the traditional identity management schemes show there is a rising need to change how we manage digital identity. Blockchain technology is an emerging technology and it is one of the possible solutions to digital identity. In this paper, some of the most popular identity management schemes based on Blockchain were reviewed. Each scheme had certain advantages and disadvantages which shows there are features that need improvement. While the schemes give more control of identity to users, human integration and user experience remains a challenge. Blockchain is a good foundation for identity management but it is not the perfect solution. The schemes need to be

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

developed further before being widely deployed. Although the application of this technology in Identity Management isn't being used extensively now, it shows potential for the future.

REFERENCES

[1] Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain", Harvard Business Review, January-February 2017 Issue
[2]P. Dunphy, F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain", IEEE Security Privacy, vol. 16, no. 4, July 2018
[3] Dirk van Bokkem, Rico Hageman, Gijs Koning, Luat Nguyen and Naqib Zarin, "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology", arXiv:1904.12816, April 2018
[4] A. Tobin, D. Reed, "The Inevitable Rise of Self-Sovereign Identity", A white paper from the Sovrin Foundation, September 2016
[5] D. Reed, Jason Law, Daniel Hardman, "The Technical Foundations of Sovrin", A White Paper from the Sovrin Foundation, September 2016
[6] A. Othman, J. Callahan, "The Horcrux protocol: A method for decentralized biometric-based self-sovereign identity", International Joint Conference on Neural Networks (IJCNN), July 2018
[7]P.L. Aublin, S.B. Mokhtar, and V. Quéma, "RBFT: Redundant Byzantine Fault Tolerance," IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), 2013, pp. 297–306
[8]A. Grüner, A. Mühle, T. Gayvoronskaya and C. Meinel, "A Quantifiable Trust Model for Blockchain-Based Identity Management," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1475-1482
[9] Z. Zheng, S. Xie, H. Dai, H. Wang, "An overview of blockchain technology: Architecture consensus and future trends", IEEE International Congress on Big Data (BigData Congress), June 2017
[10]"Hyperledger Fabric, A Blockchain Platform for the Enterprise"
[11] "What is self-sovereign Identity?", Sovrin organisation, December 2018
[12]Margaret Rouse, "Self-sovereign identity", TechTarget, May 2019
[13] Dr. C Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton, Michael Sena, "uPort: A Platform for Self-Sovereign Identity", A white paper from uPort, 2016
[14] "Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust", A white paper from the Sovrin Foundation,January 2018
[15] "Sovrin: What Goes on the Ledger?", A white paper from Evernym, 2018