Identity Management Systems Using Blockchain Technology.txt

Name:- Diwakar Kumar Yadav
College:- Institute of Engineering & Rural Technology
Prayagraj(ALLAHABAD), UP, INDIA
Gmail:- diwakarydv37@gmail.com
Linkedin:- https://www.linkedin.com/in/diwakar37/

Abstract—The emergence of Blockchain technology as the biggest innovations of the 21st century, has given rise to new concepts of Identity Management to deal with the privacy and security challenges on the one hand, and to enhance the decentralization and user control in transactions on Blockchain infrastructures on the other hand. This paper investigates and gives an analysis of the most popular Identity Management Systems using Blockchain: uPort, Sovrin, and ShoCard. It then evaluates them under a set of features of digital identity that characterizes the successful of an Identity Management solution. The result of the comparative analysis is presented in a concise way to allow readers to find out easily which systems satisfy what requirements in order to select the appropriate one to fit into a specific scenario.
Keywords— Digital Identity, Identity Management, SelfSoveriegn Identity, Blockchai

I. INTRODUCTION (HEADING 1)

In an increasingly digital ecosystem with a variety of online services, entities need to possess digital identities for their identification by allowing them to interact with each other on the online world, while protecting their identity information. 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. However, the process for identifying, authenticating and authorizing individuals to access easily different resources and services requires mechanisms to control information about individuals. Adding to the complexity of the modern identity and access management challenge, the demand for secure access poses a serious challenge for Information and Technology staff that has simultaneously to meet the access need of users and to ensure the security of their data. To overcome these demands access with a certain level of security and data protection, Identity and Access Management solutions have been introduced by which identity lifecycle is managed while allowing users to access to appropriate resources, at the right time and in the right context while saving cost and time [1]. Despite the solutions given by current Identity Management technologies to improve the management of user authentication and resources access, they still suffer from several limitations and they are not optimal to ensure data protection against abuse, fraud and criminality. Surveys conducted by the European Commission shows that people have the feeling they don't have any control over their personal data [2]. Closely related to data protection, centralized identity services that exist today fail to operate transparently and protect the rights of users. Several of these risks can possibly be avoided by using Blockchain technology [3]. A literary study made clear that this technology can add significant value in managing identities by returning the ownership of identity to the individual as an owner of this identity. Furthermore, the combination of Identity Management with Blockchain technology enables decentralized identity storage, avoids a central authentication authority and prevents tampering with the identities and the stored data. In view of all that, several initiatives put its research efforts into building consistent and robust approaches of Identity Management based on Blockchain technology with a variety of use-cases. In this paper we investigate, evaluate and compare three main Identity Management systems based on Blockchain. The structure of this paper is as follows: after this introduction, Section II defines the digital identity with its related concepts. Section III presents the evolution of digital identity models. In Section IV we give an overview of Blockchain technology. Section VI introduces current approaches related to Identity Management systems using Blockchain. It begins with an overview and a description of each system, followed by analysis and evaluations whether systems fulfill predefined requirements related to the digital identity. Section VII serves as conclusions and future work.

II. DIGITAL IDENTITY : DEFINITIONS AND CONCEPTS

Digital Identity referred to a set of information identifying uniquely an individual using digital information in order to ensure the same level of confidence that a face-toface transaction would generate. It is created in the form of specific attributes that are stored in databases and differentiate users from each other within the same system [4]. Among these attributes, there are static ones such as ethnic origin, gender, date of birth, and so on. Besides these unchangeable attributes, there are dynamic ones like age, job position, postal address and so forth. Some attributes specific to a person identifying him uniquely. This kind of attributes called identifiers such as email address, passport number, etc. Within the identity ecosystem, any identity can have many attributes, its values can be same for many users, and many identifiers, which are unique to an individual, associated with it. E-mail is the most used identifier for online services for ordinary users [5]. Figure 1 illustrates the relationship between identity, attributes and identifiers.
In addition, there are three main concepts in identity: Identity Claim: an assertion made by an individual or business. Proof: a form of document providing evidence for the claim. Attestation: the validation of the claim's correctness by a third party.

III. EVOLUTION OF DIGITAL IDENTITY MODELS

A. Typical Identity Hierarchical Models With the emerging of the digital economy with a wide web services, and to overcome the challenge of poor online registration experiences in the late 1990s, digital identity has become one of the biggest challenges for business and entities which need to provide digital identities for citizens to involve them in this interconnected environment. Thus, several models of digital identity have been introduced redefining modern concepts of identity in the digital world. In [6], authors present a description of the four typical hierarchical identity models in the current ecosystems: Conventional Model, Centralized Model, Federated Identity Model, and Users-Centric Identity Model [7]. Even if each model has its own strengths and drawbacks, all of them suffer from a common weakness which is the control of identity by central authorities which might be targets for hackers with a loss of privacy for all concerned.

B. Self-Sovereign Identity Model The conception of the digital continues to evolve and in recent years it has begun to have a new approach: selfsovereign identity (SSI) [8]. The purpose is to enhance the trust and the security, while preserving the user's privacy and protecting them from the ever-increasing control by central third parties. In other words, users are sovereigns of themself and have the full control of their identities. Christopher Allen makes a vision about self-sovereign identity with a set of features [9]which are grouped by the Soverin Foundation into three categories [10]: security, controllability and portability. The self-sovereign characteristics are:

Persistence: Identities must be long-lived as long as user wishes. Portability: information about identities must be transportable and they must not be held by a singular third party to avoid dependence on this latter. Interoperability: Identities should be as widely usable as possible, crossing boundaries while remaining user control. Consent: Users must agree to the use of their identity and the sharing of related data must only occur with the consent of them. Minimization: To enhance the privacy as best as possible, disclosure of data must be minimized and should involve the minimum quantity of data which is necessary to accomplish the required task. Protection: The right of entities must be protected, in the event of a conflict between the needs of the network and the right of users, the priority should be given to the latter.Based on the features above, a typical architecture of a SSI is usually consisting of three roles: 1) Issuer which is an individual or an organization that creates and issues claims. 2) Holder which receives holds claims and shares them selectively. 3) Verifier (third party) which receives and verifies proofs from identity holders. The identity owner can play all three roles as issuer, holder or verifier. The relationship between the different actors of a SSI model is illustrated on the figure 2.

IV. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

With the emergence of Bitcoin in 2008 by Satoshi Nakamoto [11], the technology behind the Blockchain has been raised making a huge revolution in the financial sector allowing peer-to-peer transactions of digital currency without a central authority. Ever since 2009, Blockchain technology has been expanding in a multitude of fields including government, healthcare, social media, Internet of Things (IoT), and so on. Despite this growth, the implication of Blockchain technology is still in its infancy for organizations which need to understand fundamental aspects of this technology. A. Blockchain Structure Blockchain technology is a data structure, which is represented by a list of blocks in a particular order, to establish, validate and share distributed ledger of different kinds of transactions through peer-to-peer (P2P) networks [12] of computers (nodes). It is based on cryptographic hash functions [13], asymmetric-key cryptography [14] and digital signature [15]. The architecture of Blockchain network is a set of components and concepts as is shown in figure 3. Blockchain System is composed of a number of nodes and it mainly consists of the following mechanisms:

Peer-to-peer network: Blockchain solutions are based on P2P network to exchange information between nodes using a secure broadcasting protocol [16]. Each node is involved in the propagation of transaction without any central server. This topology is the basis of Blockchain decentralized feature. Storage: To store the entire blocks of transaction replicated on each node, Blockchain technology is based on state-machine replication [17]. The decentralized storage eliminates the single point of failure so that the Blockchain system remains available despite the failure of some network participants. However, large blocks require large storage space and slower propagation in the network. Validation: this process ensures the integrity of Blockchain data avoiding issues such as double spending in crypto-currencies. Every node in the Blockchain network validates transactions against some rules by verifying that these transactions are legitimates and they have not already been spent. Then blocks consisting of valid transactions can be built [18]. Consensus: is a set of rules making all the nodes synchronized with an agreement on the transactions existence and on the state of the ledger. Several consensus processes have been proposed on Blockchain, the most common are: i) Proof - of - Work (PoW) which is based on the scarcity of computational resources where miners race to find an acceptable solution of a hard mathematical problem [19]. ii) Proof - of -Stake (PoS) which is an alternative to PoW and it is based on the scarcity of the currency [20]. Cryptography: this mechanism grants broad security and privacy to the data. Blockchain uses an asymmetric cryptography mechanism for transactions and wallets [21]. Thus, the stored data is immutable and the created blocks are impossible to be deleted or edited.

B. Classification of Blockchain Based on their permission model, Blockchain systems are categorized into three types [22] [23]: Permissionless or public Blockchains: In this category of infrastructure, anyone can join the network and begins submitting transactions without needing permission to interact with the network. This category of Blockchain has been the essence of the digital currencies market by introducing open source solutions like Bitcoin and Ethereum [24]. Permissioned or Private Blockchains: these infrastructures are closed ecosystems which require pre-verification of the participating parties within the network. Therefore, only restricted users have the rights to validate the block transactions. Permissioned Blockchains are preferred by centralized organizations to increase the control of their internal business operation. Consortium Blockchain: this kind of Blockchain is partly private where the consensus process is controlled by a selected set of participants, while the right to read Blockchain data is allowed to the public or is restricted to the participants.

V. IDENTITY MANAGEMENT ON BLOCKCHAIN

Based on the emergence of Blockchain and SSI technologies, several approaches of IDM have been raised to enhance the decentralization feature with the increasing of user identity control. In this section, we focus on three particular IDM models which have provided the required technical details of their schemes designs.

uPort [uport]is an open source platform based on SSI allowing users to register their own identities on Ethereum. The architecture of uPort consists of three key components: o Uport Mobile Application: To create a new identity and interact with Ethereum, Uport application generates an asymmetric pair key. The private key is stored on the user's device and it is never supposed to leave this latter. In the case of event of loss or theft of the mobile device, the user maintains his persistent identifier

(uPortID, 20-byte hexadecimal string). For that, the user has to nominate the uPortIDs of trustees (individuals or institutions) who can vote to replace the public key with the new one proposed by the user. o Smart contracts [25]: Uport has designed two main smart contract templates: controller contract and proxy contract. Each one includes uPortID. Whenever the user wants to interact with an application contract, from the mobile device, they send a transaction, signed by his key, via the proxy contract, through a controller contract, to the application which views the proxy contract as the sender. Besides to the controller and proxy contract, uPort system includes a registry smart contract which stores the hash of the JSON attribute structure related to the global mapping of uPortIDs to identity attributes. The data are stored in distributed file systems like IPFS, Dropbox, etc. o Developer Libraries: Describe how relying parties' developers integrate uPort into their applications.

B. Sovrin Soverin [26] is a consortium Blockchain where everybody can use the platform, without prior permission. However Sovrin is permissioned ledger with a known set of validator nodes, called stewards, which just achieve consensus on the ledger. A Sovrin identity uses decentralized identifiers (DID) [27]. The Sovrin architecture is summarized by three layers [28] as shown in the figure 5: o Sovrin Ledger: is the key component of Sovrin project. It is a distributed ledger of non-profit public organizations governed by Sovrin Foundation. the steward nodes of this ledger run The Plenum protocol which is an enhancement version of the redundant Byzantine fault tolerant protocol [29]. o Sovrin Agents: Users interact with Sovrin through agents which are acting as addressable network end points which with a high viability as other critical network services. Sovrin agents many functions in the network such as Persistent P2P messaging endpoints, coordination endpoints for multiple clients, Encrypted data storage and sharing etc. o Sovrin Clients: Applications operated on edge devices (smartphone, laptop, etc) to ensure the communication with Sovrin agents and ledger in order to conduct identity transactions.

C. ShoCard ShoCard [30], [31], [35] is a card platform enabling the creation of mobile identities to ensure a unified identification for users across different regions. The concept of this solution is the combination of the Blockchain, mobile technologies and biometrics in a federated identification system while taking into consideration the privacy and the security aspects. The ShoCard infrastructure is based on Bitcoin Blockchain and the scheme relies on three phases: o Bootstrapping: is started by the installation of the SchoCard application which generates a new asymmetric key pair for the user and scans their identity credentials using the device's camera. The data related to the user's credentials and their selfie image is encrypted and stored on the mobile device, while the hash of this data is written on the Bitcoin Blockchain as SchoCard seal associated with transactions number corresponding to the ShoCardId of the user. o Certification: after the registration phase, the user start the certification process by interacting with an Identity Provider to confirm their identity. The user provides, via a digital secured envelop, a digital link, corresponding to the user's information, to the Identity Provider which verifies the credentials against the user's entry on the Blockchain. o Validation: The validation phase occurs when a relying party must verify a certification to determine whether a user is entitled to access a service.

D. Analysis and synthesis Based on respective specifications, documentations, web pages and published papers, we have inventoried the main properties of the three Identity Management Systems as follow: uPort o User controls creation and disclosure of uPortIDs without a central authority. However, information stored in the registry may be spilled. Moreover, the JSON structure is visible to all. o Users do not need to disclose personal data for a constrained use. o Uport Supports unidirectional sharing of identifiers between Parties. o Discreet disclosure of a uPortID is possible if a user creates new uPortIDs for each new relying party that avoids the use of the registry o The usability and ShoCard privacy implications are unclear. o A mobile application is provided to interact with ShoCard infrastructure. Consistently follows a QR code scanning paradigm for all uses

Sovrin

Sovrin equips user with a full control of their identity with the possibility to choose 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. o Although there are no trusted third parties, users interact with Sovrin through a mobile application and control software agent. The agent can be run on the user's server or on specialized agencies which act on behalf of the user and they have a necessary and justifiable place in the identity relationship. o Both omnidirectional and unidirectional identifiers are supported and users may publish only identifiers and use different identifiers and cryptographic keypairs with each party they interact with.

Sovrin Foundation expects to build a market of agencies that offer agent hosting services to identity owners. o Despite all strengths of Sovrin solutions, they are not deployed widely because users found them too had to understand so that the user experience still be an issue to be addressed

ShoCard

The end-user controls the storage of his identity and the appropriate disclosure of ShoCardIDs with relying parties. o During the bootstrapping phase, ShoCard are bootstrapped with an existing document (e.g passport). Thus, more personal information are included in ShoCard seal than they had originally intended. o The ShoCard server may be able to associate a particular

ShoCardID with a particular relying party, since relying party retrieves envelopes ShoCard server. o ShoCard supports unidirectional identifiers and does not have the concept of a public registry of ShoCardIDs. o ShoCard analyses existing trusted credentials. However, for attribute validation, relying parties must create integrations with ShoCard centralized. o The usability and ShoCard privacy implications are unclear. o A mobile application is provided to interact with ShoCard infrastructure. Consistently follows a QR code scanning paradigm for all uses.
To evaluate the three currently popular Identity Management systems using Blockchain technology, we have based on the Cameron's seven laws of digital identity [36]: user control and consent, minimal disclosure for a constrained use, justifiable parties, directed identity, design for a pluralism of operators and technology, human integration and consistent experience across contexts. Based on respective specifications, documentations, web pages and published papers, Our findings, are

presented in the table I below. We have used the tick "√" to indicate that the system satisfies a respective requirement and the character "X" to indicate that the system does not satisfy the requirement. All described solutions have their special and unique properties and each scheme has its benefits and downsides. However, despite the advantages of the application of Distributed Ledger Technology to Identity Management, as evident from the table I, there is a noticeable lack of contextual understanding relating to the user experience elements, which is makes difficult for these schemes to deliver on their lofty goals. In addition, even if the main goal to adopt a Blockchain technology as infrastructure for Identity management is the removal of the central authority, this may not be a realistic goal in IdM applications due the context of identity maintaining a profound need for trust. The tightening regulatory landscape for storing personal data, for instance the law 09-08 in Morocco, grants endusers new powers over their personal data, and places new obligations upon data controllers. This creates a challenge for the design of immutable public ledgers that reference personal data, and provide inherent transparency to data that they store.

TABLE I. A COMPARATIVE ANALYSIS OF UPORT, SOVRIN AND SHOCARD

Requirements	Uport	Sovrin	shoCard
User control and consent	X	√	
Minimal disclosure for a constrained use	√	√	X
Justifiable parties	X	√	X
Directed identity	√	√	√
Design for a pluralism of operators and technology	√	√	X
Human integration	X	X	X
Consistent experience across contexts	√	X	√

VII CONCLUSION

Blockchain, as a decentralized and distributed public ledger technology in peer-to-peer network, has received considerable attention in Identity Management. In this paper we have reviewed most important concepts underlying the Identity Management and Blockchain technology. We have presented the most popular Identity Management systems using Blockchain technology: uPort, Sovrin and ShoCard. Each approach has its strengths and drawbacks. Most notably those are: more control over identity based on systems self-sovereign identity, a decentralized identity due to Blockchain and easier verification to multiple entities. However, there is a noticeable lack of contextual understanding relating to the user experience. In addition, the protection of stored data is not clear for some approaches and some privacy challenges may hinder the applications of Blockchain. Thus, efforts are required to build a more consistent view of Identity Management in order to preserve privacy when Blockchain is used.