Benefits of a blockchain-based identity management system

Dilshoda Uchqunova,
Trainee-researcher at the Research Institute
for the Development of Digital
Technologies and Artificial Intelligence
Rahmonova Madina
Trainee-researcher at the Research Institute
for the Development of Digital
Technologies and Artificial Intelligence

Abstract*. Identity management solutions are generally designed to facilitate the management of digital identities and operations such as authentication, and have been widely used in real-world applications. In recent years, there have been attempts to introduce blockchain-based identity management solutions, which allow the user to take over control of his/her own identity. In this paper, we provide an in-depth review of existing blockchain-based identity management papers. Based on the analysis of the literature, we identify potential research gaps and opportunities, which will hopefully help inform future research agenda.*

Keywords*: Identity management system, blockchain, blockchain-based identity management, self-sovereign.*

Introduction. Digital identity plays an increasingly important role in our interconnected, digitalized society. For example, most of us have a number of digital identities, associated with our workplace, our personal life, and other professional-related activity. This partly contributes to the growing reliance on identity information management, designed to manage and secure our identity information and to provide relevant services. Building on the success of blockchain, there have also been attempts to integrate blockchain in the design of

the next generation of identity management solutions [1, 2, 3]. In a typical blockchain-based identity management system, there are a large number of distributed nodes [4]. Such nodes can be utilized to provide distributed storage, reliable access and computation capabilities. The user in such a system acts as a node in the network; thus, allowing the storage of sensitive user data to shift from servers (in the conventional identity management solutions) to user devices / nodes (in the new blockchain-based paradigm). This facilitates self-sovereign identity (SSI), since the users will now have the capability to regain control of their own identity. Consequently, this minimizes various risks inherent of conventional identity management solutions [1, 2, 5].

Given the relatively recent trend in designing blockchain-based identity management solutions, it is not surprising that a number of challenges remain. For example, how can users convince organizations to willingly accept attributes of pseudonymous individuals of uncertain reputation? There are also potentially legal and financial implications, if a transaction is subsequently found to be fraudulent or criminal and the organizations have not conducted their due diligence in verifying the identity of the users involved in the transaction. We observe that self-sovereign identity is a topic that has been explored in the literature.

Therefore, in this paper we focus on the study of blockchain-based identity management systems, by reviewing recent state-of-the-art advances on the topic. Specifically, we search for relevant English-language articles and patent documents published between May 2017 and January 2020 on the various academic databases (e.g. ACM Digital Library, IEEE Explore, ScienceDirect, and Springer Link) and Google Scholar, using keywords such as (”blockchain” AND ”identity management”). Of the sixty articles found, we only include 50 articles for discussion in this paper. In Section 2, we will introduce relevant concepts of identity management and the building blocks in blockchain. Then, in Section 3, we will first introduce three existing blockchain-based identity management systems, prior to reviewing the related literature

Identity Management. As previously discussed, identity management (IdM) is also known as identity and access management (IAM) in the literature. Broadly speaking, IdM refers to a framework of policies and technologies for ensuring that only authorized individuals can access the associated resources in an organization. IdM is a relatively mature topic, given the large number of standards and frameworks [1], such as the Security Assertion Markup Language (SAML) , the Web Services Federation (WS-Fed) , the Identity Federation Framework (ID-FF) , and the Identity Web Services Framework (ID-WSF) . Examples of IdM criteria include the CoSign Protocol, the Open Authentication (OAuth) citehardt2012oauth, and the OpenID Connect (OIDC). However, as our society becomes more interconnected and digitalized, with a significant increase in the number and types of systems and identities that need to be managed, there is also a need to revisit our conventional IdM paradigms. For example, as discussed earlier, there have been attempts to leverage the characteristics of blockchain (e.g. decentralization, openness, trustworthiness, and security) in the next generation IdM design.

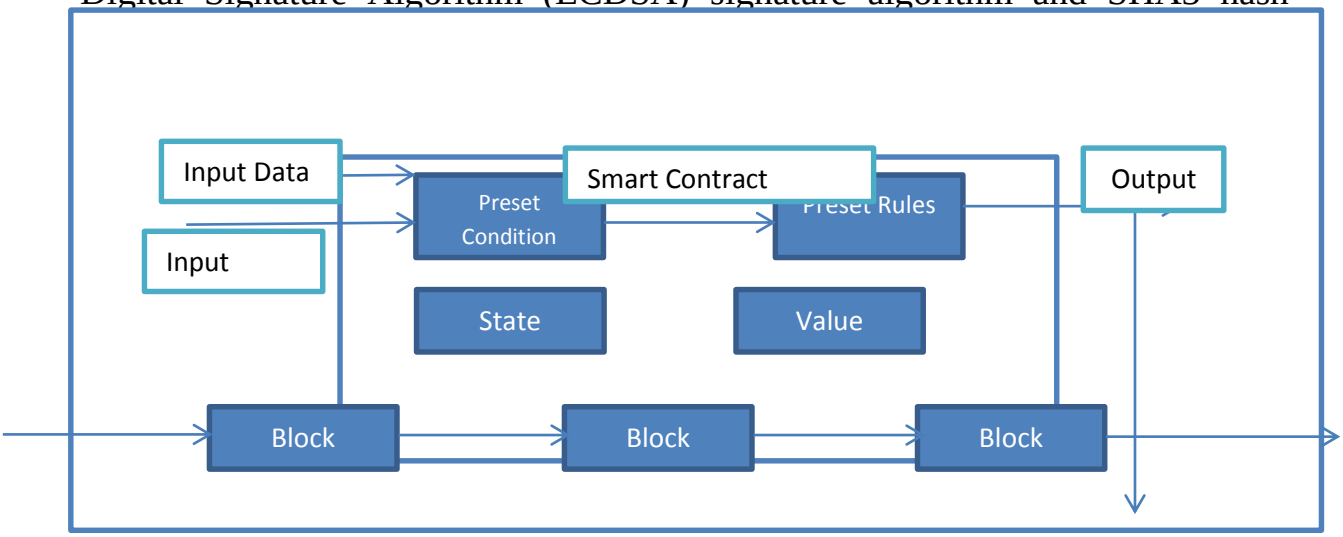
Building blocks For simplicity, let's consider the scenario where a user requests for proof of identity from an identity provider, and the identity provider responds to the token. In this simplistic setting, there is exchange of information between both entities (e.g. real individual or some entities). If the identity providers are separate entities, then this becomes a three-party identity management model of comprising users, identity providers and identity dependents. In such a model, since the identity provider is a separate entity, the identity resource used for authentication only stores in the identity provider, and the identity dependent can only verify the authentication of the user's identity by querying the identity provider. In addition to providing user identities, identity providers should also have identity management, identity reset, identity revoke, and other related functions.

• User. Users are the primary enablers of the system, enjoying the various services offered by the service provider and identity provider. Not all users have the same privilege.

• Identity provider. Identity provider, the core of the system, is tasked with providing users with identity services (e.g. registration, authentication and management). This entity also provides user authentication. • Service provider. Service provider is an important part of the system, and is mainly responsible for providing services for users (once they are successfully authenticated).

Architecture Ethereum, the first platform to run Turing complete smart contract, is currently one of the most preferred platforms for blockchain applications. Therefore, we will use Ethereum as an example to explain the blockchain architecture.

The data layer is the foundation of all functions, including data storage and security assurance. The data storage is realized through the blocks and the chain. The storage is based on the Merkle tree to ensure data persistence. Security guarantee relies on the data layer's hash function, digital signature and other cryptography technology, which collectively guarantee the security of the account and the transaction. The underlying signature and hash adopt the Elliptic Curve Digital Signature Algorithm (ECDSA) signature algorithm and SHA3 hash



The network layer is a layer implemented using peer-to-peer (P2P) technology. In a P2P network, there is no centralized server, and each user is a node with server functionality. This layer embodies decentralization and network

robustness. The consensus layer is responsible for network nodes agreeing on transactions and data, and includes two consensus mechanisms. At the beginning, there are few ethers (ETHs), and the proof of work (PoW) consensus mechanism is adopted to encourage the rapid exploration of ETHs. When the number of ETHs is sufficiently large, the proof of stake (PoS) mechanism will be adopted. Such an approach can effectively avoid the partial distribution of a single node. The network layer is a layer implemented using peer-to-peer (P2P) technology. In a P2P network, there is no centralized server, and each user is a node with server functionality. This layer embodies decentralization and network robustness.

The consensus layer is responsible for network nodes agreeing on transactions and data, and includes two consensus mechanisms. At the beginning, there are few ethers (ETHs), and the proof of work (PoW) consensus mechanism is adopted to encourage the rapid exploration of ETHs. When the number of ETHs is sufficiently large, the proof of stake (PoS) mechanism will be adopted. Such an approach can effectively avoid the partial distribution of a single node.

Table 1. Blockchain and database

CRITERIAS	BLOCKCHAIN	DATABASE
Authority	Blockchain is decentralized and has no centralized approach	Databases are controlled by the administrator and are centralized in nature
Architecture	Blockchain utilizes a distributed ledger network architecture	Database uses a client-server architecture
Data Handling	Blockchain utilizes Read and Write operations	The database supports CRUD (Create, Read, Update and Delete)
Transparency	Public blockchain offers transparency	Database are not transparent

Performance	Blockchain is bobbed down by the verification and consensus methods	Databases are extremely fast and offer great scalability
Integrity	Blockchain data supports integrity	Malicious actors can alter database data

The incentive layer is responsible for the issuance and distribution of ETHs. ETHs can be used to pay for fuel to run smart contracts, etc, and are produced by mining, with a bonus of some ETHs per block. In the smart contract layer, the running smart contract must have a corresponding virtual machine, for example, ethereum has ethereum virtual machine (EVM) to support the underlying smart contract. At the same time, the decentralized application (DAPP) has an interactive interface, which facilitates the use of smart contracts by users.

Blockchain-based Identity Management Systems

In this section, we will review three existing blockchain-based IdM systems.

• Sovrin. Sovrin is designed to use digital credentials in the offline world. Sovrin has a self-sovereign identity that does not depend on any centralized authority and cannot be eliminated. Characteristics of Sovrin include governance, scalability and accessibility. More importantly, Sovrin is a worldwide public chain based on Hyperledger that enables design privacy, such as identifying private customers under pseudonyms. It adopts zero-knowledge proof encryption to selectively ensure privacy.

• uPort. uPort is a system of self-sovereign identity. It depends on Ethereum, so the essence of the uPort identity is the Ethereum account address on which users interact, and the identity is permanent. uPort table is the smart contract for all uPort identities and is the basis for authentication and offline data access sharing. From the user's perspective, uPort optimizes Ethereum-based

applications, so that users interact with real people instead of dealing with hexadecimal addresses.

• ShoCard. ShoCard is a blockchain-based IdM system, where users can keep and protect their own digital identities. User's identity information will always be used together with the user's key to ensure privacy. This elimiates the need for a third-party database. ShoCard keeps the authentication code of user data on the blockchain, which can guarantee the legitimacy of personal identity and facilitate third-party verification. ShoCard also issues SFN coins for payments..

There are clearly many other blockchain-based IdM systems, including those proposed in the literature. In the remaining of this section, we will review the existing literature.

Conclusion. In this paper, we provided an in-depth review of blockchain-based identity management systems. As part of the review, we identified a number of challenges, such as those related to block data storage. For example, the user's storage requirement will increase with the increase of number of users and the subscribed services. Another challenge is associated with the de-authorization classification in blockchain. Some nodes can participate in book-keeping while others can only view the block data. This can potentially result in the boundary division of the chain, due to the existence of node identity.

References

[1] S. El Haddouti, M. D. E.-C. El Kettani, Analysis of identity management systems using blockchain technology, in: 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), IEEE, 2019, pp. 1–7.

[2] M. Kuperberg, Blockchain-based identity management: A survey from the enterprise and ecosystem perspective, IEEE Transactions on Engineering Management.

[3] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, K.-K. R. Choo, Best: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system, Computers and Security 85 (2019) 288 – 299.

[4] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, R. Ismail, Blockchain technology the identity management and authentication service disruptor: a survey, International Journal on Advanced Science, Engineering and Information Technology 8 (4-2) (2018) 1735–1745.

[5] A. Jindal, G. S. Aujla, N. Kumar, Survivor: A blockchain based edge-as-aservice framework for secure energy trading in sdn-enabled vehicle-to-grid environment, Computer Networks 153 (2019) 36 – 48.