An Exploratory Study on Self-Sovereign Identity Powered by the Blockchain Technology

M G Shashank, V Sangeetha and H Shilpa

May 8, 2021

An Exploratory study on Self-Sovereign Identity powered by the Blockchain Technology

Shashank M G[1], Sangeetha V[2], Shilpa H[3]

[1] PG Student, Department of Computer Science and Engineering
Ramaiah Institute of Technology, Bangalore, India
[2,3] Assistant Professor, Department of Computer Science and Engineering
Ramaiah Institute of Technology, Bangalore, India
[1]shashank30051997@gmail.com,[2]drsangeethav@msrit.edu
[3]shilpahariraj@msrit.edu

Abstract. The current state of Digital Identity Systems is fractured among service providers. Users must duplicate their identity information across services, which reduces overall accessibility and increases the likelihood of privacy breaches. Users have no knowledge of how their data is being misused by providers and they have little real influence of it. The concept of Self Sovereign Identity (SSI) has emerged, promising to usher in a new era in which the individual, and only the individual, has complete autonomy over their identity records, with clear support for a user - controlled data storage facility. With the introduction of Blockchain technology, the concept of self - sovereign identity has gained traction, and it is expected to have a significant impact on how internet users communicate in the future.

Keywords: Identity, Identity Management Systems, Self Sovereign Identity, Profile, Ethereum Blockchain, Smart Contracts, Verifiable Credentials, Distributed Ledger Technology.

1 Introduction

The term "Self-Sovereign Identity" (SSI) refers to a digital revolution that recognizes that a person can own and control their identity without the intervention of administrative authorities. People will engage in the digital world with the same independence and capacity for trust as they have in the offline world, thanks to SSI. In a secure and trustworthy scheme of identity management, self-sovereign identity takes the same independence and personal liberty to the internet. SSI denotes that a person or agency maintains and monitors access to the elements that make up their identity – digitally. In recent years, one of the most commonly used concepts in the Identity Management landscape has been self-sovereign identity. With the explosion of online services over the last fifteen years or so, managing user and service identities has risen to prominence and, in many ways, has become the foundation upon which various online services are built [1]. Self-Sovereign Identity (SSI) is a concept used to identify a digital phenomenon that respects an individual's right to own and regulate their identity without the involvement of government. As a result, it runs on a decentralized domain, and stability is paramount. The identity here not only refers to just the credentials to login and access the online services, it can also be the identity that helps us to recognize ourselves in the offline world. All those identities can be managed more efficiently with the help of Self Sovereign Identity, even without the intervention of the authority who issued us the credentials. Since Self Sovereign Identity operates on decentralized domain, Blockchain technology offers all necessary requirements to exercise the SSI to its full potential. Smart contracts are programmable pieces of code that can be executed on a Blockchain, such as the Ethereum Blockchain [2]. A solution built using Ethereum smart contracts that combines cryptographic stability, organizational independence, data autonomy, and account recoverability.

1.1 The Evolution of Identity Models

The identity management landscape has evolved in stages, beginning with the most basic model and progressing through various phases as newer models are introduced.

The Silo Model. The most general and simplest identity management approach is the Isolated User Identity (SILO) Model [18]. In this case, only two actors are involved: the service provider (SP) and its own Identity Provider (IdP), as well as the customers. Clients who choose to use a service provider's facilities are given identification and a password by the service provider. Each SP has its own identity domain, and operations performed in one don't apply to the others. When a customer wants to use a service from multiple SPs, he must go to each one and authenticate separately. All major and leading online content providers, such as Google, Yahoo, Amazon, eBay, and others, currently use this model; however, trends are shifting toward other models.

The Federated Model. Each single identity domain in the Federated model is made up of a single IdP and one or more SPs [18]. The customer receives identifiers and passwords from the IdP. The SP relies on the IdP to authenticate the user and provide the SP with user attributes and values. To use the app, users must first authenticate with the IdP, after which they will be forwarded to the service provider to use the service. After an IdP authenticates a customer, she can access resources from any service provider that uses the same IdP. The Federated Identity domain is a shared identity domain that is created once a trust relationship between the IdP and the corresponding SPs has been established.

The User Centric Model. The federated model and the user-centric model are close. A number of SPs will share a single IdP in this model, but there is no need to maintain trust among the entities [18]. When a user uses an SP to enter a program, the user is directed to the requested IdP, where she authenticates herself. The IdP then sends the user's identification data to the SP, which makes an authorization decision based on the profile to allow or deny the user's request for access to the service. Every individual in this model trusts each other and there is no concept of trust. As a result, this approach is often referred to as the Open-trust model.

1.2 The Blockchain Technology

A chain of blocks, where each block contains unchangeable records is called as a Blockchain [13]. It works as a Distributed Ledger Platform (DLP) and includes the platform's rules as well as a ledger of all transactions since the start. This technology of Blockchain offers a firm basis to understand the idea of the self-sovereign identity.

Properties of the Blockchain Technology. The first property includes Distributed Consensus, which is, the ability to reach a distributed consensus on the ledger's status without relying on a Trusted Third Party is one of the most critical features of any distributed ledger. This opens up the prospect of creating and deploying a mechanism that allows every authorized agency to verify all possible states and relationships. Immutability and irreversibility of the distributed ledger is achieved over a period of time with several nodes and distributed consensus [19]. Data in a distributed ledger is stored in a distributed manner, ensuring its persistence as long as there are nodes in the P2P network that are willing to participate. Every operation on a Blockchain is considered to be a transaction. To ensure the validity of the data source, any transaction must be digitally signed using public key cryptography. When this is combined with a distributed ledger's immutability and irreversibility, a powerful non-repudiation tool for all data stored in the ledger emerges. Hence data provenance is critical and is the fourth property. A distributed ledger ensures that data is deposited in and recovered from the ledger in a distributed, single-point-of-failure-free manner. Hence Blockchain provides Distributed data control is the fifth property. Distributed Ledger encourages openness and transparency, which is the sixth property, because the state of the ledger, as well as any single contact among participating organizations, can be validated by any approved agency [4].

1.3 The Self-Sovereign Identity

Given the amount of study being done in the area of self - sovereign identity, the introduction of Blockchain technology has heightened the interest, with multiple usage cases with various scenarios being investigated to determine the suitability of such a scheme. Even if such research is essential to advance the state of the art, one unintended consequence is that various interpretations of the word “Self-Sovereign identity" remain. It has been specified in a variety of ways in various contexts, adding to the complexity. Even though it can be used in a variety of ways depending on the situation, we believe that having a common understanding of what a self-sovereign identity is critical to realizing its full potential [1]. The synopsis of the definition highlighting the crucial properties of the self sovereign identity is quoted below [6],

‘‘*The identity belongs to the person (or organization) that* ***owns****,* ***governs****, and* ***manages*** *it entirely. In this way, the client is their own* ***identity provider****; no one else can pretend to be able to ‘‘****provide****"* ***their identity*** *because it is intrinsically theirs. You have the option of* ***revealing*** *any or all of it at any point. You can conveniently log your* ***permission*** *to share data with others to make the* ***sharing*** *easier. It is* ***tenacious*** *and* ***independent*** *of any single third party. In identity* ***transactions****,* ***claims*** *made against you can either be* ***self-asserted*** *or* ***asserted by a third party*** *whose* ***validity*** *can be objectively* ***checked*** *by a relying party. As a result, there is a type of identity that tries to strike a balance between* ***transparency****,* ***fairness****, and commons* ***support*** *while also* ***protecting*** *the individual.*"
This definition captures almost all of the properties of Self – Sovereign Identity like owing, control, manages, security etc, hence from the study of several other definitions of self sovereign identity this proves to be somewhat satisfying.

2 Related Work

MD Sadek Ferdous et al in. [1] briefly explains the way to actually define the concept of Self Sovereign Identity. Many researches conduct on SSI fails to formulate the concept of it in a definition such that on reading it is unable to get a glimpse of what SSI actually means. SSI is defined mathematically by considering the concepts of digital identity, profile, attestations, assertions, identifiers etc by formulating it in a form of an equation stating ‘SSI is the collection of partial identities of a user belonging to different decentralized domains’ [6], by a series of mathematical derivations. Getting such accurate definition of SSI helps us to exploit its full potential. The various existing Traditional Identity models have several drawbacks like user identity misuse, data breach, cyber attacks on centralized system etc. Keeping these drawbacks in mind, there are properties of SSI like transparency, security, user owner ship of data, accessibility, sharing, existence etc that shows that SSI is more secure and easy to manage user identity and its impact on the Laws of Identity [9]. The role of the Blockchain is significant as it is a distributed ledger technology with the properties like tamper proofing; consensus mechanism etc serves as a foundation upon which SSI system can be leveraged. Life cycle of SSI [10] includes registration of identity, deregistration of identity by the user, authentication, authorization and provisioning of service to the user once authenticated. Since Blockchain supports SSI, Blockchain platforms have already been exploited to develop SSI application. uPort [11] a decentralized identity system built on Ethereum platform. Jolocom [12], another SSI based application that functions similar to uPort. The use case of SSI model along with the Blockchain in a bank application explains the ease of creating the account, authenticating and access the services from the bank, because of decentralized identity system.

Komal Gilani et al in. [2] briefly explains the way in which the Blockchain based identity is a secure form of identity by specifying the various services offered by SSI to the users to protect their data. The standard process of Identity proofing and attribute assurance happens when the verifier of the credentials verifies the signature of the trusted

authorities of the credentials presented [14]. The claims are validated by verifying the signature, name, validity period and scheme. Personal data management happens by storing the claims offline and public identifier stored on the Blockchain. The Blockchain based solution helps remove the intervention of intermediaries provides privacy - enhanced identity management with scalability and optimization.
Galia Kondova et al in. [3] briefly describes that Blockchain based identity model proves to be in line with General Data Protection Model (GDPR). GDPR applies to personal data, or anything that identifies an individual. DIDs are not created by some authority but can be created by data subjects. The data subjects prove control of a DID by signing with a private key that is linked to the DID. Although DIDs are related to data subjects, they do not allow the identification unless their usage discloses the identity of the data subject. When DID is used only once, this disclosure might be limited to the information that was disclosed and does not link to additional data. DID even though created and signed by an individual sometimes the revocation of it will be under the control of identity issuer. Right to be forgotten / right to erasure is also provided by the SSI which is included under GDPR policies. Special attention has to be attributed to revocation of credentials. A revocation does not mean the deletion of the credential. It rather adds a revocation entry. This requires a legal basis. Depending on the use-case, this legal basis would often exist (but not always). SSI can provide a high standard of privacy protection. No central entity has control over the credentials issued. SSI can technically protect the privacy of data subjects and can be compliant with GDPR. However, the requirement of a case by case analysis and the existing legal uncertainty creates a burden to the use of this privacy enhancing technology.

Zachary Diebold et al in. [4] briefly explains a technical approach of implementing a Blockchain based SSI Model using Ethereum Blockchain. Ethereum Blockchain has deployed smart contracts. Their function is to store the unique user identifier, a pointer to the user's data and the logic for modifying this data. The user data is stored in JavaScript Object Notation (JSON) format on the decentralized storage platform IPFS, with a reference to this data given to the smart contract. Device key pairs are used by the users to login and update their data. Makes use of two types of contracts, identity contracts and recovery contracts. When smart contract gets deployed as a result of transaction UUID is generated for the user, with a pair of public key and private key store on Blockchain and user device respectively. The features like attribute signing, attribute disclosure and identity recovery can also be facilitated. Interaction with the Ethereum smart contracts from a browser happens with the help of Web3.js [8]. Metamask is another project for Ethereum account management that runs as a browser extension. It stores the public and private keys for Ethereum wallets in the browser local storage and supports client-side transaction signing. TestRPC can be used for rapid testing of Ethereum smart contracts and applications. It simulates a full Ethereum node and local Blockchain network. It can generate a number of addresses with initial balances and store their keys on the node. It also mines blocks of transactions instantly to facilitate faster development. An IPFS system can be used to store users' data and digital signatures during the development.

Seongho Hong and Heeyoul Kim el at in. [5] briefly explains the methodology in which the SSI model complies with OAuth 2.0 model to serve a purpose. The implementation of this Vault Point is due to the fact that each SSI model has its own authentication and authorization mechanism. This ensures that each SSI model requires users to learn a new authentication and authorization method. In addition, service developers must enforce this method separately for each SSI model in order to connect their service to the SSI models. A novel Blockchain-based SSI model is presented to address these issues. The proposed model adheres to the SSI model's concept while still complying with the OAuth 2.0 framework. OAuth 2.0 is a well-established authorization specification [15] [16] that are widely used. Since the current model is compliant with OAuth, it will not only make implementation easier, but it will also relieve users of the pressure of learning a new authentication and authorization method because they are already familiar with OAuth. User-centric authentication and authorization are allowed in the proposed model by a specification that allows each user to act as an authorization server in OAuth using their own computer. The proposed model has improved availability by allowing users to handle their information more reliably, as well as providing a decentralized authentication and authorization mechanism that is not limited to a single service provider, such as Google. The proposed model has the following contributions. First and foremost, it is the first SSI model to comply with the OAuth 2.0 specification, ensuring high reliability and interoperability. Second, it offers novel user-centric authentication and authorization that is controlled by a user's own computer using a Blockchain ledger. Third, from the perspective of service developers, the proposed model is simple to implement since it fits the OAuth 2.0 flow. Fourth, it allows a customer to handle personal information in a safe and easily available manner by encrypting it and storing it in the Blockchain.

Lesavre, Loic, Priam Varin, Peter Mell, Michael Davidson, and James Shook el at in. [20] helped in making the readers understand the emerging Blockchain Identity Management Systems using a taxonomic approach. First on explaining the various traditional identity models and listing their drawbacks like interoperability, security and privacy concerns and data leaks that occur, this paper explains the possible solutions to these issues by the introduction of Blockchain technologies in the field of identity management. Since many technologies supported by Blockchain in being introduced that supports scalability and privacy with the use of techniques like smart contracts, zero knowledge proofs etc, these systems are being designed that takes bottom-up approach or top-down approach. Those systems with the different architectural models have different control, scalability and delegation constraints. This paper examines identifier and credential structures, their use of Blockchains, and potential mixture trends. It examines the various levels at which on chain registries are established, as well as who has power over them. Bring-your-own-blockchain-address systems, as well as credentials provided as off chain artifacts, are investigated. It does not seek to compare and contrast the various architectures and models, but rather emphasizes their distinctions. This paper begins with a glossary of terms, a set of principles, and the basic components of blockchain-based identity management. The breakdown of defining properties and architectures follows. The paper then moves on to public registries and machine governance. Finally, it discusses some of the security issues that these applications can encounter, as well as additional aspects such as key blockchain protocols, zero-knowledge proofs, presentation sharing, data mining along with examples of some use cases. The aim of this paper is to help the reader understand how blockchain-based identity management systems function, what they have to offer, and how to differentiate between the various architectures and building blocks.

Baars D. S. el at in [19], in this paper a case study was included in this article, in which two parties exchanged KYC-attributes after granting express permission. The KYC attributes would be exchanged off-chain from the owner of authenticated data (issuer) to the acquirer. The transaction operation itself, as well as a signature of the information shared, will be recorded on the blockchain. The system included a Blockchain, a server application and a user smart phone application. The back end server would be connected to the Blockchain that grants permissions to user based on the data. The smart phone application is connected to the server, not directly to the blockchain. In this KYC methodology of Blockchain implementation the Bitcoin blockchain was used. This system had many advantages like key management is fully handed over to the customers, increases the trust between the organization and the user; along with few adaptation barriers since the mobile application on users phone is complex it requires a lot of explanation and also the proof of work time in Bitcoin Blockchain takes lot of time so it might take many hours before data exchange is triggered. Hence a better solution can be given using a smart contract based Blockchain like Ethereum.

Lux, Zoltán András, Felix Beierle, Sebastian Zickau, and Sebastian Göndör el at in. [21] explained how SSI is beneficial in the modern society where identity and security is crucial for every individual on the internet; it also explains that a global identification solution must be able to manage a wide range of certificate forms from millions of issuing organizations. Anyone may find appropriate and trustworthy credential forms for their use cases through looking at the documents on the Blockchain, as metadata regarding types of digital certificates is accessible for anyone on the decentralized permissioned ledger with Hyperledger Indy. Since there is currently no effective full text search system that allows users to search for credential forms in a clear and efficient manner while remaining closely embedded into their applications, this paper suggests a full text search system for retrieving matching credential forms based on publicly accessible metadata on the Hyperledger Indy ledger. Using a full-text search engine and a local copy of the ledger, the suggested approach will find credential forms based on textual feedback from the user. As a result, there is no need to depend on details regarding credentials from a vast pool of outside parties we'd have to trust, such as a company's website showing its own id and a collection of provided credentials. This paper also proves the efficiency and feasibility of this concept by the implementation of a prototype.

Dunphy, Paul, and Fabien AP Petitcolas el at in. [22] briefly explained various properties of decentralized system and also the need of DLT to implement the Identity Management System. The paper also explains various existing Self Sovereign Identity

Management Systems like uPort, ShoCard and Sovrin in detail with respect to how they are implemented, what are their drawbacks and their own benefits and advantages. Each one of them is good in its own way. In this paper uPort and Sovrin are classified under the category of Self Sovereign Identity, where as ShoCard is put under the category of Decentralized Trusted Identity. Usability is unclear, according to the article, since existing methods presume that users are familiar with DLT and cryptographic key management. They also note the lack of legislation addressing digital identities, which makes creating identification schemes difficult for businesses.

Christopher Allen el at in. [7] briefly conceptualized the various forms of Identity management systems and introduced SSI with a definition and explained the ten pillars of Self Sovereign Identity which is crucial for an SSI system to exist and operate effectively. The first pillar is Existence, stating that independent existence of users is a must. The second is the control the users have on their identity. Accessibility of user's data by the user forms the third pillar. Transparency of the system and the algorithms are crucial in an SSI system. Persistence, which forms the fifth pillar, states that the data of the users must be long-lived. Portability of the user's info across various devices and entities must be possible forming the seventh pillar. Individual's data must be portable across devices. Consent from the users to use their data must be a required feature, forming the eighth property. Minimalization and protection of data of users is a must in SSI system.

3 Discussion

In order to give an overall view of the concepts discussed, the following table [17] compare the features that exist between the traditional identity model and the SSI model and show how SSI is better.

Table 3. Comparison between several Identity Models.

	Silo Model	Federated Model	User Centric model	Self Sovereign Model
Identifiers can be generated by the Individuals	No	No	No	Yes
Individuals are in control of their own authenticators	No	No	Yes	Yes
Individuals are in control of their own digital credentials and certificates	No	No	Yes	Yes
Individuals may have power of their identifiers in the event that their keys are lost or stolen.	Yes	Yes	No	Yes

Individuals may recover their licenses and certificates if their keys are lost or stolen.	Yes	Yes	No	Yes
Individuals have access to the information that pertains to their digital identity.	Unclear	Unclear	Unclear	Yes
Zero Knowledge Proofs enabled	No	No	No	Yes
Minimization of Personal Identifiable Information (PII)	No	No	No	Yes
Guarantee of Right to be forgotten	Unclear	No	No	Yes
Authenticator and certificate repositories are portable.	No	No	Yes	Yes
Identity vendors do not maintain consolidated files containing customer information.	No	No	No	Yes
Identity companies should not have access to knowledge about people's relationships with strangers or their access to programs.	No	Yes	Yes	Yes
Regulatory regulations are followed during implementation.	Yes	Yes	Yes	Yes
Trust systems are created so that identity providers and standards of assurance can be defined.	Yes	Yes	Yes	Yes
Identity is easily retrievable in the case of a natural disaster	Yes	Yes	No	Yes
Data breaches are likely	No	No	No	Yes

4 Conclusion

With the tremendous demand for the Blockchain technology in the current era, the Self – Sovereign Identity is all set to place its foot dominantly in the field of Identity Management and Security in the upcoming years. The features of Self Sovereign Identity, such as user ownership of digital identity data, transparency, portability, availability, and persistence, are certain to revolutionize the current identity system, because traditional identity management systems pale in comparison to the level of security provided by Self Sovereign Identity for user data. The Self Sovereign Identity model can be used not just for accessing the online services or to get the user credentials verified securely, the same methodology can be applied to many areas like in banking, providing loans, e-commerce, online gaming etc. The thin line that separates user identity data and data breach or data misuse is about to be strengthened by the Blockchain and Self Sovereign Identity Technology. Many researchers are almost on their way to develop such a secure system and no doubt that building such a system requires decades of effort and constant updating. As a result, Self-Sovereign Identity can be viewed as a boon to the fields of Identity Management and Security.

References

1. Ferdous, Md Sadek, Farida Chowdhury, and Madini O. Alassafi. "In search of self-sovereign identity leveraging Blockchain technology." IEEE Access 7 (2019): 103059-103079.Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016).
2. Gilani, Komal, Emmanuel Bertin, Julien Hatin, and Noel Crespi. "A survey on blockchain-based identity Management and decentralized privacy for personal data." In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 97-101. IEEE, 2020.
3. Kondova, Galia, and Jörn Erbguth. "Self-sovereign identity on public blockchains and the GDPR." In Proceedings of the 35th Annual ACM Symposium on Applied Computing, pp. 342-345. 2020.
4. Diebold, Zachary. "Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain." Master in Computer Science. University of Dublin, Trinity College (2018).
5. Hong, Seongho, and Heeyoul Kim. "VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0." Electronics 9, no. 8 (2020): 1231.
6. Tobin, Andrew, and Drummond Reed. "The inevitable rise of self-sovereign identity." The Sovrin Foundation 29, no. 2016 (2016).
7. C. Allen, "The Path to Self - Sovereign Identity", Apr.2016.[Online]. Available: http://www.lifewithalacrity.com/2016/04/th-path-to-self-sovereign-identity.html
8. Ethereum Foundation, "Web3.js – Ethereum Javascript API." [Online]. Available: https://github.com/ethereum/web3.js.
9. K. Cameron. Microsoft Corporation. Nov. (5, 2005). The Laws of Identity. Accessed:Mar. 20, 2019. [Online]. Available: http://www.identityblog.com/stories/2005/05/13/ TheLawsOfIdentity.pdf
10. M.S. Ferdous, G. Norman, and R. Poet, ''Mathematical modeling of identity, identity management and other related topics,'' inProc. 7th Int.Conf. Secur. Inf. Netw., 2014, pp. 9–16.
11. C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena.(Oct. 20, 2016).UPORT: A Platform For Self-Sovereign Identity.Accessed: Jul. 16, 2019. [Online]. Available: http://blockchainlab.com/pdf/ _DRAFT20161020.pdf.
12. C. Fei, J. Lohkamp, E. Rusu, K. Szawan, K. Wagner and N. Wittenberg.(Mar. 9, 2018). Jolocom Whitepaper. Accessed: Jul. 16, 2019. [Online]. Available: https://jolocom.io/wp-content/uploads/2018/07/Jolocom-Technical-WP-_-Self- Sovereign-and-Decentralised-Identity-By-Design-2018-03-09.pdf
13. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2008.
14. L. Thomas., and C. Meinel, "An Attribute Assurance Framework to Define and Match Trust in Identity Attributes". IEEE International Conference on Web Services, 580-587, 2011.
15. Fett, D.; Kusters, R. A Comprehensive Formal Security Analysis of OAuth 2.0. In Proceedings of the ACMSIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019.
16. OAuth 2.0 Authorization Framework. Available online: https://tools.ietf.org/html/rfc6749 (accessed on 1 July 2020).

17. Marcos Allende López . "SELF-SOVEREIGN IDENTITY - The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain" Materials Today: Proceedings (2019).
18. M. S. Ferdous, ‘‘User-controlled identity management systems using mobile devices,’’ Ph.D. dissertation, School Comput. Sci., Univ. Glasgow,Glasgow, Scotland, 2015.
19. Baars, D. S. "Towards self-sovereign identity using blockchain technology." Master's thesis, University of Twente, 2016.
20. Lesavre, Loic, Priam Varin, Peter Mell, Michael Davidson, and James Shook. "A taxonomic approach to understanding emerging Blockchain identity management systems." arXiv preprint arXiv:1908.00929 (2019).
21. Lux, Zoltán András, Felix Beierle, Sebastian Zickau, and Sebastian Göndör. "Full-text search for verifiable credential metadata on distributed ledgers." In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 519-528. IEEE, 2019.
22. Dunphy, Paul, and Fabien AP Petitcolas. "A first look at identity management schemes on the blockchain." IEEE Security & Privacy 16, no. 4 (2018): 20-29.