A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data

Service providers continue to offer their centric solutions has serious security lacunae and is cumbersome to the users.

Challenges of IdM blockchain based
- interoperability
- trust in the management of evidences.

Komal Gilani, Emmanuel Bertin, Julien Hatin
Orange Labs, France
{komal.gilani, emmanuel.bertin, julien.hatin}@orange.com

Noel Crespi
Institut Telecom, Telecom SudParis,
CNRS UMR5157, France
noel.crespi@it-sudparis.eu

The paper provides an overview of the SSI components. It presents the IdM models and lists a set of blockchain based solutions.
Finally, the article discusses some research gaps.

***Abstract*— In the digital revolution, even secure communication between individuals, services and devices through centralized digital entities presents considerable risks. Having service providers continue to offer their centric solutions is inefficient in terms of duplication, has serious security lacunae and is cumbersome to the users. The self-sovereign Identity concept, which includes the individual's consolidated digital identity and verified attributes, enables the users of data to exert their ownership and gain insights from their data's usage. The authentication and verification of digital identity is essential to achieve the privacy and security of distributed digital identities. In this paper, we provide a coherent view of the central concepts of self-sovereign Identity, including the components of identity proofing and authentication solutions for different self-sovereign Identity solutions. We discussed an overview of Identity management approaches, introducing an architecture overview as well as the relevant actors in such a system and blockchain technology as solution for distributed user-centric identity. Finally, we discuss the existing solutions and point out the research gaps and elaborate challenges and trade-offs towards building a complete identity management system.**

***Keywords*— Blockchain, Self-sovereign Identity, authentication mechanism, Identity proofing, claim verification**

I. Introduction

Recently, the rising surveillance and security breaches concern the user's privacy in the current identity management ecosystem. To provide user-centric services, organizations assemble huge amount of personal information. The collected data is further utilized for profiling, prediction and economic growth. In many cases, the user has no insights about stored data about them and how it is used by service providers. The management of identities and personal identifies information (PII) is controlled by central authorities and user has little or no control over their data sharing and privacy. Furthermore, the collection of PII makes the service providers primary target of attacks and results in security breaches and privacy exploitation [1].

The digital identity authentication ensures that individuals are who they claim to be in the online systems. The verification of subject and protection of sensitive information is the key component of trustworthiness in the identity management. Users have to exchange their personal information with organizations in exchange of services. To overcome stealing, misusing or manipulating these data in central approach, services providers are required to provide many factor authentications along with management of identities which further complicates the systems. Besides central approach, federated instances provides access to multiple sites with same credentials. However, the control and ownership of data still remains in the hand of identity service provider.

The contemporary approaches in identity management challenge the designers for expert security reviews and usability analyses concerning user experience and interaction with active agents in the identity infrastructure [2]. The recent work to eliminate the central service providers is one unique digital identity that is build, managed and controlled by identity owner [3]. Such identity that provides user centric data ownership is called self-sovereign identity. The blockchain technology recognized as temper resistant and transparent ledger [4]. Thus, it can be used to bind the users with the claims they make to prevent the identity frauds. Besides challenges of ownership, interoperability and controllability in self-sovereign Identity, the challenge of trustworthiness by management of evidences of digital identities demands prime attention. There is significant need for protection of digital identities through standardized solutions and interfaces for identity proofing and evidence exchange between subject, claim verifier and issuer. We have formulated our discussion around the different notions of central topics in the identity management systems and blockchain technology disruption such as:

- The need to use Blockchain for identity management
- Contribution of Blockchain in digital identity
- An analysis of the existing solutions based on SSI architecture

Section II presents an overview of the identity management approach and describes the implications of managing identity using blockchain. Attribute Federation and Verified claims are discussed in section III. The related research works are presented in section IV. Section V concludes the paper with summary of the remaining issues and main challenges.

II. Background

A. Identity management approach

Identity management is an administrative process to create and maintain user account to be used for authentication and identification in online services. It is required to simplify the user provision process and ensure the rightful users can have access to the services. The identity management system (IdM in short and IdMs in plural) life cycle comprises of four phases including enrollment, authentication, issuance and verification. enrollment and the actors involved in the life cycle are Authentication Provider, Attribute Provider, Service Provider and Identity Provider. Below, we have quoted three types of IdM with or without DLT according to our interpretation.

Users have no control over their PII. The SP need to use 2 factor authn that complicates the system.

Actors of the IdM: authn provider, attribute provider, SP, IdP

General challenges of SSI
- interoperability
- trust in the management of evidences.

IdM is an administrative process to create and maintain user account for authn and authz
IdM models:
- Silo model: SP is at the center and collects users' credentials. It provides attributes.
- Federated: IdP central role (create, maintain, authn users). SP issues the service.
- SSI

The article proposes a new taxonomy of the principles of SSI, starting from the paper: "In Search of Self Sovereign Identity Leveraging Blockchain Technology"

Control is a foundamental property.

1) Silo Model: The central service provider remains the central power in this approach by collecting the user's credentials and validate them to access the online services through their own authentication mechanism [5]. In DLT bases approach users' credentials are validated through the central authority and further validation is process through identity information stored in DLT layer.

2) Federared model: An Identity provider, responsible for creating, maintaining and authenticating all users, plays the role of central hub for Various Web-based service providers [6]. User can enroll to service provider service A and can use the same identity to access the service b or any number of services allowed to be accessible through authentication process that validates the user's claim. The Facebook and Google single sign on are examples of federated entities.

3) Self-Sovereign Identity: The self-sovereign Identity provides the ownership of data to user to promote user control and transparency. Based on rules of need-to-know and need-to-retain, the owner of data can control the information without relying on third parties that can result in data lost or misuse of sensitive information. "The user's rights increased transparency with regulations, privacy by design systems, data portability and security". The importance of self-sovereign based Identity systems has skyrocketed ascribable to current identity crises. In Fig. 1, the comphrensive taxonomy of self-sovereign Identity properties is presented. We have provided our own interpretation of texanomy presented in [7]. The authory presented the taxonomy of self-sovereignity which categroized as taxanomies of foundation property, controllability property, sustainability property, security property and flexibility property. We believe the taxanomy of controability is the foundamental property of self-sovereign identity which allows the users of control, consent and disclosure.

B. Blockchain Technology

The concept of blockchain first introduced as Bitcoin [8] is a peer-to-peer network and provide transparency through reaching consensus on transactions. The immutability of blockchain and consensus role eliminate the role of central authorities and appear to be ideal solution for distributed environment. As the data is the most valuable asset today, the implication blockchain in data driven architecture can bring features of decentralization, anonymity, audibility and persistency [9]. The most frequently mentioned terms of blockchain technology are described below:

1) Node and Block: Node is computer in peer-to-peer network representing the owner of transactions carried by certain user. Block is an immutable page of distributed ledger in the blockchain. After reaching consent on transaction, a block is added in the blockchain.

2) Consensus: The consensus mechanism is used to process and validate the transaction through approval of decision of nodes. Widely used consensus algorithms include proof-of-work, proof-of-stake and Practical Byzantine Fault Tolerance.

3) Scalability: In currently available solutions, the node scalability or performance scalability is provided depending upon access. Public blockchains such as Ethereum [10] and Bitcoin provide node scalability and Hyperledger [11] as private blockchain offers performance scalability.

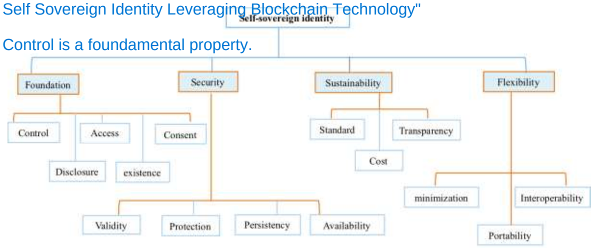

Fig. 1. Taxonomy of self-sovereign identity

4) Smart Contract: The third-generation revolution of blockchain broaden the application of blockchain in various domain besides asset management and cryptocurrency. The complex applications can be controlled by smart contract by defining arbitrary rules. The functions in Ethereum smart contract have "gas" cost depending upon computational steps and storage space. The gas cost is paid in cryptocurrency called ether.

5) Access: Depending on consensus, the blockchain is categorized into three different types. Public or permission-less blockchain provides the anonymity feature but lacks the privacy. While the private and consortium blockchain is used at organization level.

C. Motivation: Need of Blockchain

The blockchain technology coincides some interesting properties that coincides with the desirable principles of self-sovereign Identity. By leveraging the blockchain, the ten commandments of self-governed identity can be achieved to overcome digital identity issues. For instance, the consensus mechanism fulfills the need of trustworthiness for verified published attributes. As blockchain is temper-resistant ledger, the persistent of claims can be attained and forge proof storage of identities can be achieved. The SSI approach is user-centric and demand full control of user over their own data. The data stored in the blockchain is available to authorized users and owner of PII can realize full control over their data and dedicates how and what data is shared with other users.

The blockchain based chain structure that provides chain per identity such as *Trust chain* [12] or *The Tangle* [13] have been proposed to enable the full control. Such chain structure can also establish the existence principle for user to give the right to be forgotten. The claim Blocks withhold the personal information and authentication of claims ensures the protection and data minimization. The advances in the blockchain technology allows user to implement and deploy the robust and autonomous smart contracts which could be leverage to create the data sharing controller with fine-grained access control. Additionally, the blockchain technology seems promising to provide benefits of sustainability, distributed control and transparency. The interoperability and portability issue in identity management have not been addressed widely in terms of blockchain usage and it remains open issue for flexible digital identity and online services. We believe that the intervention with other technologies can more likely generate the optimal solution.

III. Attribute Federation and Verified Claims

From security perspective, solutions and regulations are developed and already concerning personal data. The exchange of information between communication agents is ambiguous and hard to keep track of what data is shared as

SC with blockchain allows data controller to fine grained access control
- interoperability issue not addressed in blockchain idm
- portability issue not addressed in blockchain idm

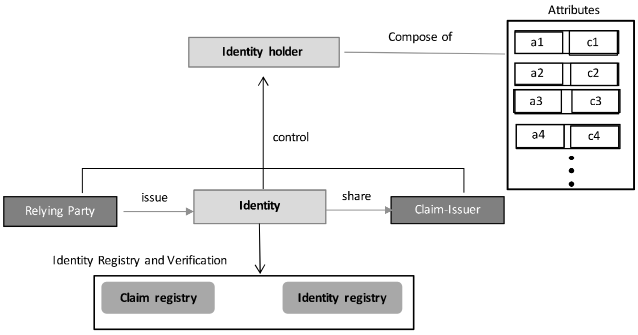

Fig. 2. Self-Sovereign identity components

compare to actual granted access. The anonymity of identity is affected by degree of link-ability of personal data [14]. As digital identity is compartmentalized into different context (personal identifiable information (PII), non-PII), It is important to provide selective disclosure of (PII) and track PII to overcome issues of personal data privacy. As mentioned in [15], PII is defined as "*subset of information sufficient to identity the identity holder within set of subjects*" such as driving license, address, passport, name, date of birth etc.

The situation and role dominate the activation of identity properties for identification and user authentication in various settings. The regulation from standard bodies are currently practiced for data privacy and management around the globe. General Data Protection Regulation (GDPR) [16] is enforced by European Union to protect consumers by returning control of their identity data back to identity holders. It includes right of access, consent, data minimization, portability and existence (right to be forgotten). The one function that is fundamental to IdM is to distinguish one subject from another. In current identity management infrastructure, service providers need to identify users through claim verification or certain attributes of the user. As shown in the Fig. 2, the subject presents the identity evidence to registration authority that inspect the identifiable information by identification information and provided identity information. The identity proofing often relies on various attributes (PII) and third party agent that demands the identity proof interacts with the identity provider . The proof is provided to relying party based on trust relationship. It is possible that user initiate the registration with identity provider without prior identity proofing and getting into identity proofing process upon concrete demand [17]. Service providers can have varying requirements for identity attributes and their quality. In this case, single trust level to an identity provider is not sufficient to assign. The multi-level trust for attributes is needed to reflect the assurance quality of different digital identities hold by an identity provider [18]. In the claim verification process, selective presentation of verification factors is essential to data protection. The subject and the verifier have to negotiate which verification factors will be used in each particular presentation and allows the subject to choose variable kinds of verification factors (e.g. credential, biometric sample and private key or PII etc.) to present to a verifier. In [19], two types of approaches are discussed for claim verification. In the first approach, named identity registry model for storage of attested claims on chain or off ledger. A claim shall include validity periods, associated identity, meta-data information and algorithm for signature/encryption and holds one to one relation with claim-issuer. A framework is proposed for [20] trust information at the identity holder as assertion as well as attribute level according to Identity, Credential & Access Management (ICAM) standard. The author in [21] also consider trust aspects of attributes more diverse and proposed to have different levels for the correctness of information subject-to-identity mapping. The identity attributes can be stored offline and hashes of certificates are stored in the blockchain upon successful verification between claim-issuer and relaying party [22]. In [23], attribute certification solution for self-sovereign Identity has been provided using blockchain. The requests of attribute certificate and certified attributes are stored in a permissioned blockchain and linked to unique user pseudonym and managed through user wallet.

IV. Overview of Identity Management Solutions

Many solutions have been proposed and developed from the perspective of digital identity management and personal data security and privacy. We limit our discussion to the systems and architectures that proposed identity management and data privacy using blockchains. There is no definitive evaluation scale available for the evaluation of proposed solutions and many of them have been evaluated and compared with other solutions based on law of identity or self-sovereign identity taxonomy. We aim to highlight the design and implementation of existing blockchain based solutions in the light of self-sovereign architecture.

The uPort [24] provides the framework for users to gather attributes from an eco-system of trust providers but does not provide identity proofing. For revocation in case of key lost, Quorum of blockchain is used. It provides data ownership and selective disclosure however the privacy of user information in JSON data structure on message server can be compromised. Jolo [25] is another self-sovereign identity management which is also developed on top of Ethereum and provide similar functions to uPort. The difference between uPort and jolo is the how the data is structure and represented in both systems.

The sovrin Foundation is a non-profile organization established to lead the global self-sovereign identity network. They have developed the sovrin IdM [26] to overcome the identity crisis through fulfilling the self-sovereign identity principles. It uses the attribute-based credentials which allows users to only reveal credentials that they choose with relying parties and WOT helps protect user against deception. For recovery mechanism, it relays on attribute-based shredding. It does not provide verification of relying parties so user needs to relay on WOT. User has full control over their identity but personal data protection is less secure as it lacks claim verification support. The adoption and integration and Sovrin standard seem constructive in novel self-sovereign identity systems. iResponder [27] is a biometric provider (based on Biometric Open Protocol Standard) that combines the biometric with blockchain technology. It offers the distributed identity to user through integration with Sovrin Foundation. The iris-scan data is stored in proprietary server and 12-digital random string serve as private key in which correspond to each unique template. In [7], the evaluation of uPort, jolo and sovrin under the comprehensive taxonomy of self-sovereign identity is analyzed. It has been shown that none

SP has different requirements for identity attributes. Needed a trust for each attestation issued.
Subject and verifier negotiate the list of attributes required.

Blockchain-based idm

uPort provides the framework for users to gather attributes from an eco-system of trust providers but does not provide identity proofing. For revocation in case of key lost, Quorum of blockchain is used.

Sovrin: It uses the attribute-based credentials which allows users to only reveal credentials that they choose with relying parties

Challenges of IdM blockchain based
- flexibility (only in blockchain). This should guarantee backward compatibility. Transfer of minimum data to other platforms.
- scalability

of the existing systems fulfill the requirements of flexibility need of digital identity for the heterogenous online service. EverID [28] is another IdM that leverage the biometric to verify user's identity/ It provides personal data ownership in hands of identity-owner and provide control of data sharing and data usage. This system is an integration of everID and everWallet (a digital wallet) which is used to store documents. The user can create the everID and use it to upload their documents and third parties can provide attestation via signatures.

The shoCard [29] provides verification of identity for online interaction and use stored encrypted version of attribute certificate on server as backup. It uses the central server as intermediate between user and relying parties. However, data minimization is not supported well. It uses Bitcoin to record a commitment to personal data that was verified during identity proofing, and store the hashes of certifications that build upon the user's seal created by relying parties. The sovrin identity system facilitate with identification on permissioned ledger. Blockstack [30] attempts to redesign the naming system in order to provide elucidation of Identity. It has PKI authentication features using state machines and storage aspect in blockchain to preserve privacy and resource identification. In Selfkey [31], users can verify the identity and access multiple service. The Selfkey digital wallet is used to digital id (public/private key) and user can access their digital id attributes and other locally stored documents through wallet. The public key is shared across the network and used to receive attestation for documents from other parties. It is compliant with KYC (know your customers by design. In Civic [32], the credentials are encrypted and stored on the digital wallet on the mobile device. User and verifying parties can check the validity of the attested claims by the flag indicating the expiration status. It voids flexibility and transparency of digital identity since the third-party mobile phone wallet is used for storage. The technical evaluation of above-mentioned solutions is presented in Table I.

V. Research Challenges and Trade-offs

We have discussed the self-sovereign identity architecture and various blockchain based identity solutions that claims to fulfill the self-sovereignty. Blockchain technology can disrupt the traditional approach of identity management and this intervention can benefit the self-sovereignty vision of digital identity. The ongoing research in this domain includes implementation of proof of concept for proposed solutions based on principle of self-sovereign identity that now act as evaluation criteria. However, the need of open standards, network scalability and flexible identity, adoption of novel solutions and user empowering identity objectives such as giving full control have been highlighted. These concerns are much needed to be addressed in future novel solutions or as enhancement in existing solutions. Below, we have explained these challenges and trade-offs in building a feasible and effective IdM. In this section, we point out few future challenges.

- Elimination of Intermediaries: Each blockchain-based IdM offers the decentralized solution to alleviate the control of centralized authorities. However, most of these solutions relies upon central server or intermediaries for data storage and key revocation. More so, the complete removal of CA can compromise several functions of identity management such as backup of cryptographic keys, identity recovery, lookup services etc. It has been shown in the practice that user consent often leads to disclosure of maximum information as they are habitual to the different warnings [2]. It is very crucial to address the questions such as: Does the users able to securely manage their own identity? Are more choices beneficial for the users in practice? In such situations, users can partially rely on other service for management of identity.

All blockchain based solutions rely on intermediaries to store data. Removing the CA compromises functions of identity recovery, pki, etc...

- Scalability and Optimization: Currently, many proposed novel solutions for IdM using blockchain are either prototypes or developed systems with promised scalability in future research. The scalability and optimization aspects for distributed IdM is essential to uptake adoption to avoid considerable delay in specific use cases such as identity verification for digital visa system or payment verification.
- Trust Required: The trust and reputation between attestation verifiers and relying parties is essential to certify identity attributes in WOT where any node can

TABLE I. TECHNICAL EVALUATION OF IDMS

IdM	Network	Key Management	Data storage	Selective Disclosure	Smart Contracts	Trust Required	Auth	GDPR compliant
Sovrin/ iResponder	Public Permissioned	DPKI (Decentralized Public Key Infrastructure)	On/off Ledger	Yes	No	Yes	No	Yes
Civic	Public	Wallet	On/off Ledger	Yes	Yes	No	No	?
Self-Key	Public	Wallet or External	Off-Chain Store	Yes	Yes	No	No	KYC compliant
uPort	Public	User Device and DPKI	Off-Chain Store	Yes	Yes	No	No	?
Blockstack	Private	DKM ((Decentralized Key Management)	Existing storage	Yes	Yes	No	Yes	?
ShoCard	Public	DPKI	Off-Ledger	No	No	No	Yes	?
Jolocom	Public/Private	HD keys (Deterministic keys)	On/off Ledger	Yes	Yes	No	No	?
EverID	Private	Wallet /Biometric Data	On/off Ledger	Yes	Yes	No	No	Yes

voucher others and it becomes difficult to quantify the trust anchors in the network.

- Privacy-enhancing identity management: As the user controlled identity demands transparent flow of data, identity management infrastructure should be designed to support pseudonymity while maintaining required degrees of confidentiality, integrity, authenticity, nonrepudiation and robustness. In an authorized access to certain service as an anonymous user, identity holder needs to show authorizations to the service which are issued by a third party while they remain unlinkable to the users' pseudonyms. The verification of third parties and mechanism to build trust relationship between service provider and third parties needs secure communication channel.

- Flexibility: To ensure the interoperability in the real-world applications, the backward compatibility is much needed. The integration of blockchain based IdM with existing solutions can initiate rapid acceptance in the market as compare to novel solutions. The research and technical work around portability of the digital identity must be taken into consideration. It must ensure the smooth transfer with minimum identity data of identity to other platform when existing platforms disappear due to some reasons.

- User experience: The user experience and human integration is another challenge needs to be addressed by DLT based IdM. The research in usability and user experience of identity management is still in incipient stage and seems to lack the vision of long-term span. The wide adoption of federated identity management by users suggest that novel solutions for identity management built upon same user interaction unlikely to uptake [33]. The authentication and identity proofing methods merely relay on unique identification through blockchain identifier and poor management of private keys by users limit the scope of IdM for non-technical users. The design of IdM must be based open standards and established protocols to ensure maximum transparency and adoption.

REFERENCES

[1] V.Goel. Facebook tinkers with users' emotions in news feed experiment, stirring outcry. The New York Times, 2014.

[2] R.Dhamija and L.Dusseault, 'The Seven Flaws of Identity Management: Usability and Security Challenges', IEEE Secur. Priv., vol. 6, no. 2, pp. 24–29, Mar. 2008.

[3] A.Abraham, Self-Sovereign Identity, Styria: E-Government Innovationszentrum; Graz University of Technology, 2017.

[4] O.Jacobovitz. Blockchain for identity management., https://www.cs.bgu.ac.il/ %7Efrankel/TechnicalReports/2016/16-02.pdf, 2016.

[5] A. Jøsang and S. Pope. User-Centric Identity Management. In Andrew Clark., editor, *Proceedings of AusCERT 2005*, Brisbane, Australia, May 2005.

[6] Chadwick, D. W. (2009). Federated identity management. In *Foundations of security analysis and design V* (pp. 96-120). Springer, Berlin, Heidelberg.

[7] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in *IEEE Access*, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017

[10] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.

[11] Foundation, T.L., Hyperledger Overview. 2018.

[12] P. Otte, M. de Vos and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain", Future Generation Computer Systems, vol. 107, pp. 770-780, 2020. Available: 10.1016/j.future.2017.08.048.

[13] S.Popov: "The tangle", 2015.

[14] S.Clauß, D.Kesdogan, T.Kölsch, Privacy enhancing identity management: protection against re-identification and profiling. In: Proceedings of the 2005 workshop on Digital identity management. DIM '05, ACM, pp 84–93, 2005

[15] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management A Consolidated Proposal for Terminology," version v0.25, December 2005

[16] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," A Practical Guide, 1st Ed., Cham: Springer International Publishing, 2017

[17] M. Onik, C. Kim, N. Lee and J. Yang, "Privacy-aware blockchain for personal data sharing and tracking", Open Computer Science, vol. 9, no. 1, pp. 80-91, 2019. Available: 10.1515/comp-2019-0005.

[18] 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

[19] Mühle, A. Grüner, T. Gayvoronskaya and C. Meinel, "A survey on essential components of a self-sovereign identity", Computer Science Review, vol. 30, pp. 80-86, 2018. Available: 10.1016/j.cosrev.2018.10.002.

[20] L.Thomas, and C.Meinel.: "Enhancing Claim-Based Identity Management by Adding a Credibility Level to the Notion of Claims," Services Computing, IEEE International Conference on, pp. 243-250, 2009 IEEE International Conference on Services Computing, 2009

[21] A.Bhargav-Spantzel : "Protocols and Systems for Privacy Preserving Protection of Digital Identity", PhD Thesis (2007). http://www.gradschool.purdue.edu/downloads/ETDForm9- E2.pdf, 1-222.

[22] Stokkink, Quinten and Pouwelse, J.A, "Deployment of a Blockchain-Based Self-Sovereign Identity. 1336-1342. 10.1109/Cybermatics_2018.2018.00230., 2018

[23] P.Coelho, A.Zúquete, and H.Gomes, "Federation of Attribute Providers for User Self-Sovereign Identity Journal of Information Systems Engineering & Management, 3(4), 32,2018.

[24] C.Lundkvist, R.Heck, J.Torstensson, Z.Mitton, and M.Sena, 'uPort: A Platform for Self-Sovereign Identity'. 21-Feb-2017.

[25] C. Fei, J. Lohkamp, E. Rusu, K. Szawan, K. Wagner and N. Wittenberg. (Mar. 9, 2018). *Jolocom Whitepaper*. Accessed: Jul. 16, 2019.

[26] Tobin and D. Reed, "The inevitable rise of self-sovereign identity," The Sovrin Foundation, 2016.

[27] *Irespond.org*, 2020. [Online]. Available: https://www.irespond.org/. [Accessed: 07- Jun- 2020].

[28] 'Travel Identity of the Future – White Paper'. SITA; ShoCard, May-2016

[29] B. Reid and B. Witteman, "Everid whitepaper," EverID, techreport, May 2018, [Accessed: 4 - mar - 2019].

[30] M.Ali, J.C.Nelson, R.Shea, & M.J.Freedman, "Blockstack: Design and Implementation of a Global Naming System with Blockchains", 2015

[31] SelfKey, "Selfkey," The SelfKey Foundation, Tech. Rep., Sep. 2017, [Accessed: 4 - mar - 2019].

[32] Civic Technologies, "Civic Token Sale WhitePaper," accessed March 26, 2019.

[33] P. Dunphy and F. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain", IEEE Security & Privacy, vol. 16, no. 4, pp. 20-29, 2018. Available: 10.1109/msp.2018.3111247.