The University of Texas at Austin
Center for Identity

# On the Usability of Self Sovereign Identity Solutions

*Razieh Nokhbeh Zaeem*
*Manah M. Khalil*
*Michael R. Lamison*
*Siddhartha Pandey*
*K. Suzanne Barber*

*UTCID Report #21-02*

August 2021

# On the Usability of Self Sovereign Identity Solutions

Razieh Nokhbeh Zaeem
University of Texas at Austin
Austin, Texas, USA
nokhbeh@utexas.edu

Manah M. Khalil
Michael R. Lamison
Siddharth Pandey
Verizon
Dallas, Texas, USA
{manah.khalil,michael.lamison,siddharth.pandey}@verizon.com

K. Suzanne Barber
University of Texas at Austin
Austin, Texas, USA
sbarber@identity.utexas.edu

## ABSTRACT

In the absence of a unique identity layer on the Internet, many identity solutions have evolved over time—examples include standalone username and password pairs, Single Sign On, and Federated Identity Management. Privacy and security risks for identity owners and liability for identity issuers and verifiers, however, are still alarmingly present. Self-Sovereign Identity (SSI) solutions are new technologies that recognize the need to keep user identity privately stored in user-owned devices, securely verified by identity issuers, and only revealed to verifiers and relying parties as needed. Many commercial SSI solutions are already available to users, issuers, and verifiers. As other researchers have pointed out, usability remains a pressing unknown in the existing SSI solutions. We study five of the most commonly used SSI solutions: uPort, Connect.me, Trinsic, Jolocom, and ShoCard (now PingID) with respect to their usability. We identify some concrete usability problems and suggest ways to resolve them. Our work recognizes that identifying, prioritizing, and implementing the non-functional requirement of usability in SSI solutions is essential for their adoption.

## CCS CONCEPTS

• **Computer systems organization** → **Peer-to-peer architectures**; • **General and reference** → *Surveys and overviews*; • **Security and privacy** → **Access control**; **Authentication**; **Authorization**; **Privacy protections**; **Usability in security and privacy**.

## KEYWORDS

self-sovereign identity, blockchain, distributed ledger technology, usability, privacy

## 1 INTRODUCTION

Identity proofing–that is, verifying an individual is who they claim they are–is required in many online and off-line activities. Unfortunately, no unique identity layer exists on the Internet. To fill this vacuum for online identity proofing, a haphazard structure has evolved over time, which includes standalone user-names and passwords, Single Sign On (SSO), and Federated Identity Management by third parties (e.g., Google and Facebook). The lack of uniform standards and methods for online Identity Management (IdM) has led to privacy risks, security vulnerabilities, risks for identity owners, and liability for identity issuers and relying parties. Self-Sovereign Identity (SSI) solutions and similar forms of IdM on the blockchain Distributed Ledger Technology (DLT) are novel technologies that emphasize the need to keep user identity privately stored in user-owned devices, securely verified by identity issuers, and only revealed to verifiers and relying parties as needed.

Academic researchers have studied SSI basics, proposed new SSI solutions [13, 24, 32], and evaluated the existing ones [7, 11, 25, 33, 43]. Nonetheless, commercial implementations of SSI solutions largely precede the academic work (e.g., Evernym [10] was started in 2012, ShoCard [31] in 2015, and uPort [39], Sovrin [35], and Civic [5] in 2016). Indeed, part of the optimism toward the potential widespread adoption of SSI is due to the very fact that commercial solutions already exist and appear to be thriving.

Like any other commercial software solution, SSI solutions must be usable and human-meaningful to gain adoption. Provability, Interoperability, Portability, Pseudonymity, Recovery, Scalability, Security, and *Usability* are the most prominent non-functional requirements of SSI, widely recognized in the academic literature and also in the commercial and open-source solutions and standards (e.g., Rebooting Web of Trust, the W3C Credential Community Group, the Decentralized Identity Foundation, and the Internet Identity Workshop).

SSI solutions, however, are heavily technology-oriented. They take advantage of sophisticated cryptography, peer-to-peer networks, and the distributed ledger technology. Researchers have already pointed out that in SSI "[u]ser interfaces are effective if they hide underlying complexity, such as cryptographic operations, biometric mechanisms, database access, and protocols." [36] Some of the most prominent papers on SSI identify usability as "a particularly pressing unknown" [7]. Some have gone as far as to say "there is a sense that a technically focused development community is overlooking the inevitable user experience and accessibility issues" of SSI [23].

In this work, we perform a preliminary analysis of the top existing commercial SSI solutions to evaluate their usability. We make the following contributions:

- We investigate the top five existing SSI solutions with respect to usability: uPort [39], Connect.me [6], Trinsic [37], Jolocom [19], and ShoCard (now PingID) [31]. Many academic papers identify these solutions as the top five existing solutions [3, 7–9, 16, 20, 22, 26, 40].
- We highlight usability pitfalls which seem common across these solutions.
- We propose ways to improve their usability with respect to the identified pitfalls.

SSI solutions and concepts offer decentralization, immutability, transparency, and security. Our work seeks to improve the usability of SSI solutions so that these solutions can indeed enjoy widespread use. Our hope is that SSI does not become a heavily technological

solution (of cryptography and distributed ledger technology) in search of a problem. Identifying, prioritizing, and implementing the non-functional requirement of usability in SSI solutions paves the way for their adoption.

We organize the rest of this paper as follows. In Section 2 we cover basic fundamentals of SSI and then briefly review the five solutions we investigate in Section 3. Section 4 explains the usability issues we found and elaborates on some potential ways to resolve them. Finally, Section 5 concludes the paper.

## 2 BACKGROUND

The term **blockchain** was coined by the Bitcoin white-paper [27]. That work pioneered a new crypto-currency (i.e., electronic cash), which would allow online transactions go through without relying on a trusted financial third party. Two major components of the blockchain technology are: (1) a peer-to-peer distributed network and (2) asymmetric key encryption. The parties of the financial transaction communicate through digital signatures (i.e., public and private keys). The peer-to-peer network timestamps transactions by hashing them into a chain of blocks, building a record of transactions. The longest chain of blocks (hence named blockchain) serves as a tamper-proof ledger of all witnessed transactions and cannot be altered without the consensus of the network majority.

The blockchain technology has found many applications [4, 12, 18, 21, 38], **including blockchain-based Identity Management (IdM)**, patient IdM [17] and the Internet of Things IdM [2, 15, 42]. An IdM is the framework that identifies, authenticates, and authorizes users to access resources. In any IdM, the identity owner (user) makes identity claims (i.e., asserts something about his/her identity) to an identity verifier (relying party). To prove this claim the user provides an identity credential as an evidence, which should be attested (i.e., validated) by the relevant identity authority (i.e., the identity issuer). Blockchain-based IdM solutions [29, 34, 41, 43] adopt blockchain for identity management to offer decentralization, immutability, transparency, and security [7]. The asymmetric encryption component of the blockchain provides authenticity of the identity proof and attestation. The peer-to-peer network component eliminates the need for a central repository of users' identity.

Today, there are two types of blockchain-based IdM solutions [7]:

- Decentralized Identity (e.g., ShoCard) is like the conventional digital identity management solutions wherein credentials from a trusted service are required. The difference from conventional solutions arises when validated attestations are stored on the blockchain.
- Self-sovereign identity (e.g., uPort, Connect.me, Trinsic, and Jolocom) allows the user to keep their identity documents in their own device. The user device creates a public/private key pair and contacts identity issuers to associate and attest their public key with an identity credential—saving the association on the blockchain. When the user makes a claim, he/she signs the claim with the private key of the attested public key. The verifier retrieves the public key from the blockchain and accepts only the claims signed with the corresponding private key.



## 3 THE FIVE SSI SOLUTIONS INVESTIGATED

In this section we briefly introduce the SSI solutions we studied. We used the Android app available on Google Play Store as of June 28, 2021.

### 3.1 uPort

uPort [39] is a "[s]elf-sovereign identity and user-centric data platform on Ethereum" [39], a public permissionless blockchain. The uPort project first began in 2015 and contributed to may SSI libraries. It later evolved into an open source project named Veramo and sought to deprecate its mobile app in June 2021. We were, however, still able to download and install it from Google Play on June 28, 2021.

### 3.2 Connect.me

Connect.me [6] is a digital identity solution that allows its users "hold all kinds of useful things, [g]et digital credentials, share them easily when needed." [6]. Connect.me is built by Evernym on top of Sovrin which uses a public permissioned blockchain. The Connect.me app is available on Apple App Store and Google Play.

### 3.3 Trinsic

Trinsic [37] claims to be "the proof of anything platform" [37]. Based on Hyperledger Aries and Sovrin (public permissioned blockchain) projects, Trinsic provides Software Development Kits (SDKs) for developers and a wallet for identity users.

### 3.4 Jolocom

Jolocom [19] is a small company in Germany which provides digital identity solutions. Jolocom uses the public permissionless Ethereum as its blockchain.

### 3.5 ShoCard

ShoCard (now acquired by PingID) [31] lets users "take full control over [their] data by sharing only what [they] want with others, while keeping [their] personal information securely stored on [their] mobile device." [31]. ShoCard is a decentralized identity solution as explained in Section 2. ShoCard uses the (permissionless) Bitcoin blockchain [1].

## 4 USABILITY PITFALLS

One of the major pitfalls we observed was how commonly all the five studied SSI apps (also known as wallets) relied on QR code scanning to initially connect an identity owner with an issuer or a verifier. Figure 1 shows the main page of the Connect.me app and how scanning a QR code is an integral part of the main use-case. The use of QR codes is suboptimal when it comes to usability: not all identity owners are present in the same physical location with the intended issuer/verifier to scan the QR code. As a workaround, the issuer or verifier usually asks the identity owner to go to a website by entering a URL and then scan the QR code from the website. However, the mere task of entering the website URL could have been used in lieu of scanning the QR code, eliminating one step in the process.

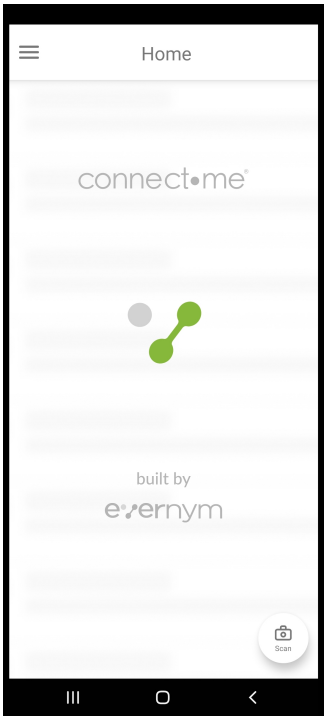


**Figure 1: A screen-shot of the main page of the Connect.me app, and its button to scan a QR code.**

We brainstormed some new ideas to replace the QR code when applicable:

(1) NFC tags, similar to the way payment is done with mobile wallets today, could detect the proximity of the identity owner device and the issuer/verifier device. The issuer/verifier may send a push notification to the identity owner. This solution unifies the ID wallet with the credit card wallet, improving usability even further.
(2) The issuer/verifier may read a sequence of characters to the identity owner (e.g., over the phone) that would act as a substitute to the QR code. Voice recognition may make entering this sequence even easier.
(3) a DNS-like system may be used to look up names. Therefore, the user simply enters a registered name of the issuer or verifier, the way URL names are entered today. The DNS-like system looks up the QR codes for the user.
(4) When migrating from an old-fashioned physical identity (like a passport), simply scanning the existing old-fashioned credential could connect to the credential provider.

Another usability pitfall we found was when it comes to backup and recovery of identity credentials. Previous work found that many existing SSI solutions simply lack the option to allow the user to back up and eventually recover their identity (e.g., after loosing a device) [28]. Among the solutions we studied, all five provide such options for backup and recovery. However, many use a seed of (commonly) 12 words. The user saves, writes down, or memorizes a sequence of words and later utilizes those words to recover a lost identity. Surprisingly, Jolocom has bugs in its software (the Jolocom SmartWallet app for Android[1]) stopping successful recovery. We think that using these seeds is not the most usable way for backup and recovery. Other researchers have identified seed keeping as a usability issue too [30].

To improve the usability of backup and recovery, one might imagine using a combination of biometrics (e.g., fingerprint and iris scan). However, more nuances are involved. The recovery of an identity should work, among other use cases, once the device is permanently lost. While the user still maintains their biometrics, the device which recorded them is lost so a comparison cannot be made unless the biometrics are save somewhere outside of the device, that is on the blockchain. Storing biometrics on the blockchain is, to say the least, very controversial. Some even believe that "[b]iometrics, in its raw or derived form (templates), should never be stored (plain or encrypted) on a public distributed ledger system." [14].

Another potential solution to the usability of backup and recovery is to allow users more control in the selection of their seed, leading to ease of remembering the seed, while still enforcing strong combinations of words. Finally, the user may go to identity issuers in person, the way one applies for a driver's license today, to have their lost identities restored.

## 5 CONCLUSIONS

SSI solutions can particularly improve their usability. In this work, we reviewed the current literature on the usability of the existing SSI solutions and investigated five of the most commonly used SSI solutions. We highlighted two tangible issues with their usability: (1) the less-than-ideal nature of having to scan QR codes in most of the use-cases, and (2) the difficulty to back up and recover an identity. We recommended ways to improve SSI solution usability with respect to those issues. On the way to revolutionize digital identity, usability is a must, and that is true, especially, for technologically-heavy SSI solutions.

## ACKNOWLEDGMENTS

The University of Texas Center for Identity wishes to thank Verizon for its collaboration, leadership, and sponsorship in this research. This research is funded in part by Verizon, Inc.

## REFERENCES

[1] Jamila Alsayed Kassem, Sarwar Sayeed, Hector Marco-Gisbert, Zeeshan Pervez, and Keshav Dahal. 2019. DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Applied Sciences* 9, 15 (2019), 2953.
[2] Paulo C Bartolomeu, Emanuel Vieira, Seyed M Hosseini, and Joaquim Ferreira. 2019. Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 1173–1180.
[3] Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. 2019. Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access* 7 (2019), 164908–164940.
[4] Christian Cachin and Marko Vukolić. 2017. Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873* (2017).
[5] Civic. [n.d.]. Civic Decentralized Reusable KYC Services - Blockchain-Powered. https://www.civic.com/solutions/kyc-services/.
[6] Connect.me. [n.d.]. Connect.me. https://connect.me
[7] Paul Dunphy and Fabien AP Petitcolas. 2018. A first look at identity management schemes on the blockchain. *IEEE Security & Privacy* 16, 4 (2018), 20–29.

[1] That bug is now fixed in version 2.0.0

[8] Samia El Haddouti and M Dafir Ech-Cherif El Kettani. 2019. Analysis of identity management systems using blockchain technology. In *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 1–7.

[9] Jørgen Ellingsen. 2019. *Self-Sovereign Identity Systems: Opportunities and challenges*. Master's thesis. NTNU.

[10] Evernym. [n.d.]. Evernym. https://www.evernym.com

[11] Md Sadek Ferdous, Farida Chowdhury, and Madini O Alassafi. 2019. In search of self-sovereign identity leveraging blockchain technology. *IEEE Access* 7 (2019), 103059–103079.

[12] T. M. FernÃąndez-CaramÃĺs and P. Fraga-Lamas. 2018. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* 6 (2018), 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

[13] Zhimin Gao, Lei Xu, Glenn Turner, Brijesh Patel, Nour Diallo, Lin Chen, and Weidong Shi. 2018. Blockchain-based identity management with mobile device. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. 66–70.

[14] Paco Garcia. 2018. Biometrics on the blockchain. *Biometric Technology Today* 2018, 5 (2018), 5–7.

[15] Samson Kahsay Gebresilassie, Joseph Rafferty, Philip Morrow, Liming Luke Chen, Mamun Abu-Tair, and Zhan Cui. 2020. Distributed, Secure, Self-Sovereign Identity for IoT Devices. In *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. IEEE, 1–6.

[16] Andreas Grüner, Alexander Mühle, Tatiana Gayvoronskaya, and Christoph Meinel. 2019. A comparative analysis of trust requirements in decentralized identity management. In *International Conference on Advanced Information Networking and Applications*. Springer, 200–213.

[17] Bahar Houtan, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis. 2020. A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access* 8 (2020), 90478–90494.

[18] Marco Iansiti and Karim R Lakhani. 2017. The truth about blockchain. *Harvard Business Review* 95, 1 (2017), 118–127.

[19] Jolocom. [n.d.]. Jolocom. https://jolocom.io

[20] Galia Kondova and Jörn Erbguth. 2020. Self-sovereign identity on public blockchains and the GDPR. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. 342–345.

[21] Karim R Lakhani and M Iansiti. 2017. The truth about blockchain. *Harvard Business Review* 95 (2017), 118–127.

[22] Yang Liu, Debiao He, Mohammad S Obaidat, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, et al. 2020. Blockchain-based identity management systems: A review. *Journal of Network and Computer Applications* (2020), 102731.

[23] Mick Lockwood. 2021. An accessible interface layer for Self-Sovereign Identity. *Frontiers in Blockchain* 3 (2021), 63.

[24] Kumaresan Mudliar, Harshal Parekh, and Prasenjit Bhavathankar. 2018. A comprehensive integration of national identity with blockchain technology. In *2018 International Conference on Communication information and Computing Technology (ICCICT)*. IEEE, 1–6.

[25] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. A survey on essential components of a self-sovereign identity. *Computer Science Review* 30 (2018), 80–86.

[26] Atif Ghulam Nabi. 2017. Comparative study on identity management methods using blockchain. *University of Zurich* 118 (2017).

[27] Satoshi Nakamoto. 2019. *Bitcoin: A peer-to-peer electronic cash system (2008)*. Technical Report. Manubot.

[28] Razieh Nokhbeh Zaeem, Kai Chih Chang, Teng-Chieh Huang, David Liau, Wenting Song, Aditya Tyagi, Manah M. Khalil, Micheal R. Lamison, Siddharth Pandey, and K. Suzanne Barber. 2021. Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study. (2021). Under Submission.

[29] Rima Rana, Razieh Nokhbeh Zaeem, and K Suzanne Barber. 2019. An Assessment of Blockchain Identity Solutions: Minimizing Risk and Liability of Authentication. In *2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI)*. 26–33.

[30] Martin Schäffner. 2019. Analysis and evaluation of blockchain-based self-sovereign identity systems. *Master's thesis* (2019).

[31] ShoCard. [n.d.]. ShoCard. https://shocard.com

[32] Reza Soltani, Uyen Trang Nguyen, and Aijun An. 2018. A new approach to client onboarding using self-sovereign identity and distributed ledger. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 1129–1136.

[33] Quinten Stokkink and Johan Pouwelse. 2018. Deployment of a blockchain-based self-sovereign identity. In *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. IEEE, 1336–1342.

[34] Makoto Takemiya and Bohdan Vanieiev. 2018. Sora identity: Secure, digital identity on the blockchain. In *2018 ieee 42nd annual computer software and applications conference (compsac)*, Vol. 2. IEEE, 582–587.

[35] Andrew Tobin and Drummond Reed. 2016. The inevitable rise of self-sovereign identity. *The Sovrin Foundation* 29 (2016).

[36] Kalman C Toth and Alan Anderson-Priddy. 2019. Self-sovereign digital identity: A paradigm shift for identity. *IEEE Security & Privacy* 17, 3 (2019), 17–27.

[37] Trinsic. [n.d.]. Trinsic. https://trinsic.id

[38] Sarah Underwood. 2016. Blockchain beyond bitcoin. *Commun. ACM* 59, 11 (2016), 15–17.

[39] uPort. [n.d.]. uPort. https://www.uport.me

[40] Fennie Wang and Primavera De Filippi. 2020. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Frontiers in Blockchain* 2 (2020), 28.

[41] Razieh Nokhbeh Zaeem and K Suzanne Barber. 2020. How Much Identity Management with Blockchain Would Have Saved Us? A Longitudinal Study of Identity Theft. In *International Conference on Business Information Systems*. Springer, 158–168.

[42] Xiaoyang Zhu and Youakim Badr. 2018. Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors* 18, 12 (2018), 4215.

[43] Guy Zyskind, Oz Nathan, et al. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*. IEEE, 180–184.

WWW.IDENTITY.UTEXAS.EDU