INTERNET POLICY REVIEW
Journal on internet regulation

Self-sovereign identity
Volume 10 **Issue** 2

GLOSSARY ENTRY

OPEN ACCESS

PEER REVIEWED

Self-sovereign identity

Alexandra Giannopoulou *University of Amsterdam* a.giannopoulou@uva.nl
Fennie Wang *Dionysus Labs* fennie@dionysuslabs.com

DOI: https://doi.org/10.14763/2021.2.1550

Published: 20 April 2021
Received: 18 April 2021 **Accepted:** 24 April 2021

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Giannopoulou, A. & Wang, F. (2021). Self-sovereign identity. *Internet Policy Review*, *10*(2). https://doi.org/10.14763/2021.2.1550

Keywords: Identity

Abstract: The concept of self-sovereign identity (SSI) describes an identity management system created to operate independently of third-party public or private actors, based on decentralised technological architectures, and designed to prioritise user security, privacy, individual autonomy and self-empowerment.

This article belongs to the **Glossary of decentralised technosocial systems**, a special section of *Internet Policy Review*.

Definition of the term

The concept of self-sovereign identity (SSI) [1] describes an identity management system created to operate independently of third-party public or private actors, based on decentralised technological architectures, and designed to prioritise user security, privacy, individual autonomy and self-empowerment.

Origin

Bringing Westphalian state-centred sovereignty to the individual level, SSI emerged from the aspiration of self-determination and of direct *self-governance* (Orgad, 2018, p. 253) for each individual, outside state intervention. Identity is considered foundational for promoting social equality, freedom, democracy, and financial independence (Verhulst & Young, 2018). Originally, *self-sovereign authority*—the ideological progenitor to SSI—referred to '*the actual default design parameter of Human identity, prior to the "registration" process used to inaugurate participation in Society. The act of "registration" implies that an administration process controlled by Society is required for "identity" to exist. This approach contrives Society as the owner of "identity", and the Individual as the outcome of socio-economic administration*' (The Moxy Tongue, 2012). Autonomy is viewed as a determining element of self-sovereignty, ideologically aligning with transcendentalism. According to Trotter (2014, p. 245), '*each of us is owned by the state, which grants leeway (...) to govern and dispose of certain aspects of our bodies and lives*'.

In the race towards digital sovereignty, i.e. '*the ability of individuals to take actions and decisions in a conscious, deliberate and independent manner*' (Pohle & Thiel, 2020) aiming to establish control '*over their data, device, software, hardware, and other technologies*' (Couture & Toupin, 2019, p. 12), identity management is key. Identities and their respective technological infrastructure vices begin to merge, while becoming a resource for the global economy: biometrics are turning into governmental infrastructures and are associated with state-issued identifiers and citizen IDs establishing citizenship (Lyon, 2008). Behavioural identity is derived from consumer personal data, collected and monetised by private actors. Technical identities are formed by local access control IDs. Health identities start to appear

[1] We will use the term sovereign identity and SSI interchangeably.

as immunity passports. Financial identity escapes financial institutions and generates value in *fintech* (Westermeier, 2020). Situated within broader digital identity development discussions [2] (United Nations, 2015), control over identity becomes instrumental as individuals, state, and private actors compete for power over its physical and digital expressions.

The concept of SSI has been elaborated as an expression of personal digital sovereignty by Christopher Allen (2016). He used it to describe a principle-based framework that would create a decentralised system of user-centric, self-administered, interoperable digital identities. This system is driven by ten foundational principles, following Kim Cameron's Laws of Identity (2005): 1) Existence, 2) Control, 3) Access, 4) Transparency, 5) Persistence, 6) Portability, 7) Interoperability, 8) Consent, 9) Minimalisation, 10) Protection, that would aim to constitute the (missing) "identity layer" on the internet (Preukschat & Reed, 2021). It embodies a specific vision of decentralised digital identity, separated from pre-existing centralised and federated models, which aims to decouple identity issuance by the state in order to bring it to the full control of the citizen (The Moxy Tongue, 2016). At the minimum, SSI '*makes the citizen entirely responsible for the management, exploitation and protection of one's data*' (Herian, 2019, p. 115). While implementations of its principles vary substantially, it can be said that SSI aims to '*enable a model of identity management that puts individuals at the center of their identity-related transactions, allowing them to manage a host of identifiers and personal information without relying upon any traditional kind of centralized authority*' (Renieris, 2020). This does not imply that the actors responsible for issuing elements of one's identity will be stripped from their privilege [3], but rather that an individual in possession of more identifiers can present all claims correlated to those identifiers '*without having to go through an intermediary*' (Wagner et al., 2018, p. 9).

Evolution

The use of SSI has been tied to the use of a blockchain. However, SSI is blockchain-adjacent, but not blockchain-dependent. As Cheesman points out, '*[s]ome bemoan the conflation of "true SSI" with ill-defined concepts such as "user-centric" digital identity, which may not require blockchain technology or use it to its full imagined, decentralised potential.*' (2020, p. 6).

The technical dimension of SSI has so far been anchored in *decentralised identifiers*

[2] According to goal 16.9 of the United Nations 2030 Agenda for Sustainable Development, the objective is to 'provide legal identity for all, including birth registration' by 2030.

[3] In that regard, it distances itself from the concept of sovereignty (Manski & Manski, 2018).

(DID), *verifiable claims* (VC) and other related standards from the World Wide Web Consortium (W3C), the same internet standards organisation behind the common internet protocols we are familiar with today such as HTML and HTTPS. These decentralised identity standards are a set of technical standards for linking and associating data about an identity-subject together in a persistent and universal manner, such that the identity-subject not only has control over how information is linked and used, but is the owner of the profile, rather than a third-party service provider. Thus, the set of linked data, called attestations or claims, may be globally portable. Attestations may include credentials that grant the identity-subject access rights or privileges, or may include verification of information such as a link to identity documents, professional certifications, credit history, or any other data or information. Every attestation that is linked to an identity-subject must be signed digitally by another identity-subject.

SSI systems may be compatible with a blockchain for documenting and attaching the transactions to each identity-subject's profile. The blockchain would record transactions that include the adding or signing of attestations, the granting or revocation of access privileges, and so on. The blockchain documentation creates a record of the data integrity of a set of information linked to an identity-subject.

SSI hinges on the technical efficiency of its core concepts. For instance, no two people should have the same identifier (*unicity*), whereby the identifier cannot reference more than one identity-subject. This condition can be satisfied through the use of cryptography, i.e. mathematically ensuring that only unique identifiers are issued and preventing them from being reissued. In other cases, such as voting or credit checks for cross leverage, no one person should have more than one identifier (*singularity*), whereby the relationship between the identity-subject and identifier is one-to-one only. This condition may be the most challenging in a pseudonymous and decentralised identity system. In a world which requires singularity of identification, technical tools and/or legal requirements that are exogenous to an SSI system appear to be a solution. The singularity quality of an identifier and identification system has traditionally been solved through centralised databases, wherein all sources of information can be aggregated to one authority that can cross check whether one identity-subject has multiple identities and identifiers (Wang & De Filippi, 2020).

Coexisting uses/meanings

As described above, SSI is oftentimes used interchangeably with terms such as decentralised identity and digital identity. While the first two terms refer to a rather similar identity management system, one that applies technological architectures such as the ones mentioned above guided by political and ideological agendas, digital identity represents a broader techno-legal societal shift towards incorporating physical identity values in a digital form. It is supported by a network of legal reforms, and facilitated by technological developments (Sullivan & Berger, 2017).

The management of (physical and digital) identity is subject to national regulation, as an expression of digital state sovereignty (Madiega, 2020). On a European level, several initiatives have been launched with a focus on digital identity services. In its recent communication, the European Commission mentions that '*a universally accepted public electronic identity (eID) is necessary for consumers to have access to their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily sharing personal data with them. Europeans can also benefit from use of data to improve public as well as private decision-making*' (2020a, p. 11). The 'Digital Finance Strategy for the EU' specifies that '*by 2024, the EU should implement a sound legal framework enabling the use of interoperable digital identity solutions*' (2020b, p. 5), which would bring technological standardisation, interoperability, and broader security in customer/user identification and authentication by financial institutions.

According to the Commission, the promotion and regulation of digital identity is essential in maintaining an *'open, democratic, and sustainable society'*, which is one of the main objectives of this data strategy. For this, trusted and secure interactions are essential. The objective would be to ensure appropriate and interoperable identification and authentication frameworks. Current digital identity reforms are often aligned to SSI for their objective to create user-centric data sovereignty. However, and as pointed out by Sheldrake, '*although SSI has been scoped, architected and built as technology, it is not merely technology. By definition, it is sociotechnology'* (2020, n.p.).

Issues currently associated with the term

While there have been considerable reforms that have facilitated the proliferation of (private/public) identity solutions, there remain numerous legal compliance shortcomings in the implementation and generalised adoption of decentralised (self-sovereign) identity.

Specifically, the eIDAS Regulation defines different levels of trust services and provides the regulatory environment that enables the creation of numerous interoperable digital identity solutions (Alamillo, 2020; Schroers, 2018). According to Article

3, electronic identification is '*a material and/or immaterial unit containing person identification data and which is used for authentication for an online service*'. Any form of cross-border digital identity (self-sovereign or not) would have to function within a mutually recognised identity framework between EU member states for authentication and access to electronic services.

In addition, identity providers have to conform to data protection regulation such as the GDPR (Renieris, 2020; Giannopoulou, 2020). Compliance appears to be rather challenging, due to constraints related to the governance, architecture, and the technological design of the identity project. For instance, actor liability of decentralised architectures remains uncertain (Finck, 2019). Similarly, the exercise of data subjects' rights within a self-sovereign identity architecture has yet to be tested, especially with the emergence of new types of trust actors.

Many applicable legal norms are sector-specific. In financial regulation, the Payment Services Directive 2 aims to facilitate financial data sharing in order to expand the technological abilities of the existing financial infrastructures (Westermeier, 2020) and to '*promote innovative mobile and internet payment services*'. Identity and the use of strong authentication technological standards are both key in applying and implementing the aspirations of the European legislator within the financial sector. This is also apparent when reviewing *anti money laundering* (AML) and *know your customer* (KYC) obligations, revised by the AML5 Directive, which require a digital identity that facilitates transparency and accountability of financial intermediaries. The application of these obligations in the broader cryptocurrency network of actors remains unclear.

Public discourse highlights SSI's foundational goal of placing the identity subject in control of their identity data [4] (user-centric identity), and views SSI solutions as a much needed global infrastructure that would provide documentation to large populations that have none, better integrating them in modern digital society (World Bank Group, 2018; World Economic Forum, 2018). However, there are considerable risks related to the expansion of global SSI systems for purposes such as refugee identification. As pointed out by Cheesman (2020, p. 14), '*the emancipatory potential of decentralised, user-owned modes of identification came into tension with the geopolitical reality of the nation-state system in which states' prerogative is to control the legitimate means of movement – or, indeed, identification*'. The persistent integration of an identity layer cannot account for anonymity nor for the contextual,

[4] This objective is perfectly aligned with the ideals of decentralisation that drove the development of blockchain technology in general (Bodó & Giannopoulou, 2020).

interpersonal nature of most expressions of our identity (Hopman & M'Charek, 2020). Following a tradition of identification technologies, ' *intensified regimes of surveillance, securitisation and control'* (Lyon, 2008; Cheesman, 2020) would tend to emerge, further solidifying existing inequalities (Gstrein & Kochenov, 2020).

There is a rapidly flourishing digital identity market, with previously isolated technological infrastructures converging, and enabling the circulation and commodification of identity-data. While often lauded, the commodification of identity by various private identity providers (Birch, 2014) could result in states competing in an open market for (sovereign) citizens. Finally, as reputation (Mac Sıthigh & Siems, 2019) is becoming essential in producing trust within modern platform-mediated digital services (Bodó, 2020), decentralised identity is regarded as an equalising force between power asymmetries. However, lately, new intermediaries have started to emerge in the field of *decentralised reputation systems*, and with them, comes the potential for a new societal order of surveillance (Foucault, 2004), defined by the consequences of assigning persistent identities to control financial, criminal, and human flows.

Conclusion

Self-sovereign identity (SSI) is rooted in the belief that individuals have the right to an identity independent of reliance on a third-party identity provider, such as the state or any other central authority. Its implementation requires the development of technical standards, as well as socio-political adaptations rooted in legal amendments in order to be successful. Overall, SSI is implemented as blockchain-adjacent, but not blockchain-dependent identity management systems, which are guided by the fundamental principle of user-centric design, using technical standards that enable user-generated and user-controlled decentralised identifiers, associated credentials, and attestations. This is supplemented by legal and policy requirements to ensure that the objectives for particular use cases are achieved, including balancing competing societal goals between user privacy, security, law enforcement, financial inclusion and risk management.

References

Alamillo Domingo, I. (2020). *SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market?* [Report]. European Commission. https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-legal-report

Allen, C. (2016, April 25). The path to self-sovereign identity [Blog post]. *Life With Alacrity*. https://w ww.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html#dfref-1212

Birch, D. (2014). *Identity is the new money, london publishing partnership*.

Bodó, B. (2020). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*. https://doi.org/10.1177/1461444820939922

Bodó, B., & Giannopoulou, A. (2020). The logics of technology decentralization: The case of distributed ledger technologies. In M. Ragnedda & G. Destefanis (Eds.), *Blockchain and web 3.0: Social, economic, and technological challenges routledge*. https://doi.org/10.4324/9780429029530-8

Cameron, K. (2005, May). The laws of identity [Blog post]. *Kim Cameron's Identity Weblog*. https://www.identityblog.com/?p=352

Cheesman, M. (2020). Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics*. https://doi.org/10.1080/14650045.2020.1823836

European Commission. (2020a). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions on shaping Europe's digital future, COM(2020) 67 final*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0067

European Commission. (2020b). *Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions on a digital finance strategy for the EU. COM/2020/591 final*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591

Finck, M. (2019). *Blockchain regulation and governance in europe*. Cambridge University Press. https://doi.org/10.1017/9781108609708

Foucault, M. (2004). *Sécurité, Territoire, Population*. Gallimard.

Giannopoulou, A. (2020). Data Protection Compliance Challenges for Self-sovereign Identity. In J. Prieto, A. Pinto, A. K. Das, & S. Ferretti (Eds.), *Blockchain and Applications* (pp. 91–100). Springer International Publishing. https://doi.org/10.1007/978-3-030-52535-4_10

Gstrein, O., & Kochenov, D. (2020). Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world? *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2020.00010

Herian, R. (2019). Regulating Blockchain. Critical perspectives in law and technology. *Routledge*. https://doi.org/10.4324/9780429489815

Herian, Robert. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156–174. https://doi.org/10.1080/17579961.2020.1727094

Hopman, R., & M'Charek, A. (2020). Facing the unknown suspect: Forensic DNA phenotyping and the oscillation between the individual and the collective. *BioSocieties*, *15*, 438–462. https://doi.org/10.1057/s41292-020-00190-9

Lyon, D. (2008). Biometrics, identification and surveillance. *Bioethics*, *22*(9), 499–508. https://doi.org/10.1111/j.1467-8519.2008.00697.x

Mac Sıthigh, D., & Siems, M. (2019). The chinese social credit system: A model for other countries? *Modern Law Review*, *82*(6), 1034–1071. https://doi.org/10.1111/1468-2230.12462

Madiega, T. (2020). *Digital sovereignty for Europe* (Briefing PE 651.992; EPRS Ideas Papers). European

Parliamentary Research Service.

Manski, S., & Manski, B. (2018). No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World. *Law and Critique*, *29*(2), 151–162. https://doi.org/10.1007/s10978-018-9225-z

Orgad, L. (2018). Cloud communities: The dawn of global citizenship? In R. Bauböck (Ed.), *Debating transformations of national citizenship*. (pp. 251–260). Springer. https://doi.org/10.1007/978-3-319-92719-0_46

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity. Decentralized digital identity and verifiable credentials, MEAP*.

Renieris, E. (2020). SSI? What we really need is full data portability [Blog post]. *Women in Identity*. https://womeninidentity.org/2020/03/31/data-portability/

Schroers, J. (2018). The final piece of the eIDAS Regulation [Blog post]. *KU Leuven Centre for IT & IP Law*. https://www.law.kuleuven.be/citip/blog/the-final-piece-of-the-eidas-regulation/

Sheldrake, P. (2020, October 19). *The dystopia of self-sovereign identity*. Generative Identity. https://generative-identity.org/the-dystopia-of-self-sovereign-identity-ssi

The Moxy Tongue. (2012, February 15). What is 'sovereign source authority'? [Blog post]. *The Moxy Tongue*. https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

The Moxy Tongue. (2016, February 9). Self-sovereign identity [Blog post]. *The Moxy Tongue*. https://www.moxytongue.com/2016/02/self-sovereign-identity.html

Trotter, G. (2014). Autonomy as self-sovereignty. *HEC Forum*, *26*, 237–255. https://doi.org/10.1007/s10730-014-9248-2

United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. https://sdgs.un.org/2030agenda

Verhulst, S. G., & Young, A. (2018). *Field report on the emergent use of distributed ledger technologies for identity management* [Report]. The GovLab. https://blockchan.ge/blockchange-fieldreport.pdf

Wagner, K., Némethi, B., Renieris, E., Lang, P., Brunet, E., & Holst, E. (2018). *Self-sovereign identity. A position paper on blockchain enabled identity and the road ahead* [Position paper]. Identity Working Group of the German Blockchain Association. https://www.bundesblock.de/wp-content/uploads/2018/10/ssi-paper.pdf

Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion, frontiers in blockchain. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2019.00028

Westermeier, C. (2020). Money is data – the platformization of financial transactions. *Information, Communication & Society*, *23*(14), 2047–2063. https://doi.org/10.1080/1369118X.2020.1770833

World Bank Group. (2018). *Identification for Development Annual Report* [Report]. https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018_ID4D_Annual_Report.pdf

World Economic Forum. (2018). *Identity in a digital world—A new chapter in the social contract* [Report]. World Economic Forum. http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Published by

Alexander von Humboldt
INSTITUTE FOR INTERNET
AND SOCIETY

in cooperation with

CREATe

centre
internet
et societe

UOC
R&I
IN3
Internet
interdisciplinary
Institute
Universitat Oberta de Catalunya