



Delft University of Technology

Governance and societal impact of blockchain-based self-sovereign identities

Gans, Rachel Benchaya; Ubacht, Jolien; Janssen, Marijn

DOI

[10.1093/polsoc/puac018](https://doi.org/10.1093/polsoc/puac018)

Publication date

2022

Document Version

Final published version

Published in

Policy and Society

Citation (APA)

Gans, R. B., Ubacht, J., & Janssen, M. (2022). Governance and societal impact of blockchain-based self-sovereign identities. *Policy and Society*, 41(3), 402-413. <https://doi.org/10.1093/polsoc/puac018>

Important note

To cite this publication, please use the final published version (if applicable). Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights. We will remove access to the work immediately and investigate your claim.

Governance and societal impact of blockchain-based self-sovereign identities

Rachel Benchaya Gans , Jolien Ubacht and Marijn Janssen

Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands
Corresponding author: R. Benchaya Gans, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands. Email: r.benchaya-gans@tudelft.nl

Abstract

Traditionally, governments and companies store data to identify persons for services provision and interactions. The rise of self-sovereign identities (SSIs) based on blockchain technologies provides individuals with ownership and control over their personal data and allows them to share their data with others using a sort of “digital safe.” Fundamentally, people have the sole ownership of their identity data and control when and how it is shared, protecting their privacy. As these data need to be validated to be trusted, they may become a more important data source for digital information sharing and transactions than the formal source of identity controlled by governments. Furthermore, SSIs can be used for interacting digitally with any organization. These developments change the relationship between government, companies, and individuals. We explore information sharing and governance in the digital society using blockchain-based SSIs. In addition, the impact of SSIs on data storage in the digital world is assessed. Technology enactment might result in no greater control or privacy and might only reinforce current practices. Finally, we argue that regulation and a combination of centralized and decentralized governance are still required to avoid misuse and ensure that envisaged benefits are realized.

Keywords: self-sovereign identities; blockchain; technology enactment; governance

Humans have sought ways to determine their identity since ancient times. From simply appointing names to objects or their peers, establishing an identification has been a genuine human kind's need. Stryker & Burke (2010, p. 284) argued that “the common usage of the term identity belies the considerable variability in both conceptual meanings and its theoretical role.” People identify themselves through their political views, from the religious group they belong to, from their place of birth or residency, or their social and economic group. Therefore, “identity” is defined differently and from various perspectives.

The legitimization of the political power and, consequently, the endorsement of the government's authority on the identification of its citizens validate the centralization of this process. Traditionally, the government is the sole authority with legal competence to testify the being's legal existence and, therefore, to issue an identification document, such as a passport. This reality implies that the government gathers citizens' personal information and safeguards it. More recently, private enterprises have also played a role in collecting their customers' data via online transactions.

However, through technological innovations and its disruptions, government and civilians' power asymmetry is also changing. While in the past, citizens needed to prove their identity mainly for civil bureaucratic matters, in the digital era, a person's authentication is required for many different types of objectives, and a formal paper identification is not sufficient anymore. A person can interact on

the Internet as a citizen or a consumer, therefore holding multiple identities. Identities are crucial for interacting securely and safely in the digital world. This has resulted in a move of power to companies storing a big amount of data about persons, resulting in an unbalance. Companies can use the data for all kinds of purposes. This power unbalance has given rise to the General Data Protection Regulation (GDPR).

Online interactions with commercial organizations and the advance of digital governmental services spurred the need for digital identities. However, so far, these forms of digital identities did not diverge a lot from the traditional papers of the past. The power to maintain citizens' data remained in the hands of the government. Primarily identification and authentication services are introduced to enable transactions with the government. Identification is the ability to identify a citizen uniquely, whereas authentication is the ability to prove that a citizen or application used by the citizen is genuine and belongs to the person that claims to be.

For example, in the private sector, companies need to check the identity to verify the age of somebody who wants to buy alcoholic drinks. Traditionally, a passport, driver's license, or identity card is shown to verify the age. Also, companies need identity when selling/buying products to ensure that a payment will be made and the products delivered. For this, the identities of the transaction parties need to be known, and their signatures are required in order to create a legal agreement.

These efforts merely replicate the conventional activities in the digital world. More recently, with the implementation of blockchain-based self-sovereign identities (SSIs), the power of citizens' data management shifted. The SSI reflects the distributed nature of distributed ledger technology (DLT), which is at the heart of blockchain. SSI enables citizens to control their data and share these with others. Hence, there is a shift from the government as a steward for their identity data to the citizens who control their own identity data. A shift has the potential to have a major impact on the relationship between governments and their citizens. SSI empowers individuals with ownership of their private data, enabling the data owner to decide which purposes and when to share their information securely via blockchain technology. Yet, citizens can potentially use these SSIs in their role as consumers to interact with private companies.

Governments will need to develop new or adapt their existing policies to these developments and ensure sound governance to warrant public values, in which privacy, transparency, inclusiveness, and the protection of the vulnerable are among them. The way the technology will be adopted impacts society. Governance focuses on guiding the mutual shaping and co-creation of technology and society (Ulnicane et al., 2020). Therefore, this study investigates information sharing and governance in the digital society using blockchain-based SSI and the possible impact on society and seeks to answer the following question:

What are the governance and societal impacts of blockchain-based SSIs?

This article is structured as follows: The Theoretical Background demonstrates the theoretical background and discusses the development of models for digital identification, namely centralized, federated, and SSI. Moreover, the analysis of the various perspectives of identities is presented. This section also examines the social relevance of a formal identification as one of the Sustainable Development Goals of the United Nations (SDG-UN) and how SSIs can contribute to achieving this target. The "Identity perspectives section" describes the challenges of adopting SSI in the policy and governance domains and the concepts of governance by blockchain, SSI governance, and shift in power balance based on the technology enactment framework (TEF). Furthermore, examples of SSI pilots and their implications on society are discussed in Policy and governance challenges on the adoption of SSI, and, finally, the conclusions and suggestions for further research are drawn in in the end.

Theoretical background

Development in data storage for identification

Since the advance of the Internet, the way governments perform their role has changed. From a paper-based to a digital services delivery environment, digital life became a reality for governmental affairs. The cyber transformation has disrupted the traditional identification and authentication process concerning individuals' data storage—a primary governmental role. Traditionally, a user is authorized with an identity and corresponding keys in which all users' personally-identifying information is centralized stored (Xu et al., 2020). The centralized authentication results in a single point of failure and makes it vulnerable to attacks and misuse.

Lips (2006, p. 2) argued that the verification of the identity is at the core of government service provision and that the process “sets within a traditional environment of trust (...) supplemented by a face-to-face assessment of the citizen by the official, based upon the citizen’s appearance of honesty or upon the official’s knowledge of the citizen within the local community.” However, this centralized identity management method is sensitive to data breaches, identity theft, and fraud (Aydar & Ayvaz, 2019). Furthermore, the concentration of information might result in possible abuse by the government, and, as a consequence, there should be measures against it (Janssen & van den Hoven, 2016). The situation of undocumented migrants reflects this concern: the fear of the anti-immigration laws and deportation and the abuse of information by governments are among their fears (Benchaya Gans et al., 2020).

What in the past was a truly “repositories of stored paper records” (Lips, 2006, p. 1) with citizen’s data, now the data storage became digital and yet seriously vulnerable to cyber attacks. Online data storage is prone to security breaches and does not always comply with users’ privacy needs (Janssen & van den Hoven, 2016). Due to centralized databases’ vulnerability and attractiveness, nationwide identity theft has already happened.

Beyond governmental matters, private enterprises increasingly collect personal data from their customers, as “data is undoubtedly the oil of the information society, almost every big company wants to collect data as much as possible, for their future competitiveness” (Wang et al., 2019, p. 1). For every online transaction in which users are requested to create an account, they need to share their personal data. Storing data in large centralized databases makes them vulnerable and attractive to hackers. There are many examples of stolen identity data. There are equally websites for checking if your data have been stolen (e.g., <https://HaveIBeenPwned.com>).

Identity management systems (IdMs) are subject to requirements of privacy laws like the European Union Directive on Data Protection, called the GDPR (Clauß & Köhntopp, 2001), which provides users with the legal grounds to decide to which extent their data are shared. It also enables them to revoke access to their data and the right to correct their personal data stored in the IdMs. The GDPR also requires the secure storage of data and the reporting if the data are accessed by unauthorized persons or stolen. Both the regulator and affected persons need to be informed in this case.

The developments in IdMs focus mainly on addressing issues related to information security and the necessity to allow the users the control of their data, avoiding information leakage, identity theft, and privacy offense (Birrell & Schneider, 2013). Figure 1 shows IdMs evolution to improve the protection of private data. The literature describes these developments (Centralized Identity Management, Federated Identity Management, and SSI Management; Birrell & Schneider, 2013; Gilani et al., 2020; Naik & Jenkins, 2020).

With the advance of the Internet, organizations need to know the identity of their users. For this purpose, IdMs were introduced, which are operated by a single organization in a centralized manner in which a single authority takes control and acts as the identity provider (Birrell & Schneider, 2013; Dhamija & Dusseault, 2008; Dunphy & Petitcolas, 2018).

In Figure 2, the working of a centralized IdM is schematically shown. In these systems, to avoid data misuse, four phases are required to ensure the protection of information, named enrollment, authentication, issuance, and verification (Gilani et al., 2020). Facebook Single-Sign-On is a classic example of a centralized IdM (Birrell & Schneider, 2013). To ensure that the right persons could be authenticated, more and more information is collected about an individual. This information enabled the organization to check if a person was genuine. At the same time, more data can be stolen once the IdM is hacked.

Eventually, the alternative of Federated identity systems has emerged, as shown in Figure 3. Federated identity systems “link attributes in users’ service provider accounts (...) without centrally storing personal information. Federated identity management would enable individuals to interact with various service providers or websites with trust relationships by signing in just once” (Shim et al., 2005, p. 120). As this definition claims, the implicit element in federated IdMs is trust (Chadwick, 2013), as entities use the same identification data to connect to a network and secure access to private users. Federated systems avoid the duplication of information in many systems. Yet, there is still centralized storage, which creates vulnerability, and the user is not in control of their own data but depends on the federated identity provider.

Finally, in a more contemporary view, blockchain-based SSIs propose strengthening decentralization and transparency while giving users control of their personal data. Instead of providing consent

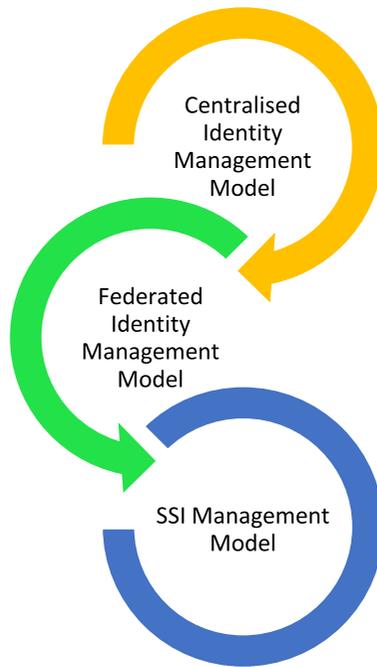


Figure 1. Development of management models for digital identification.

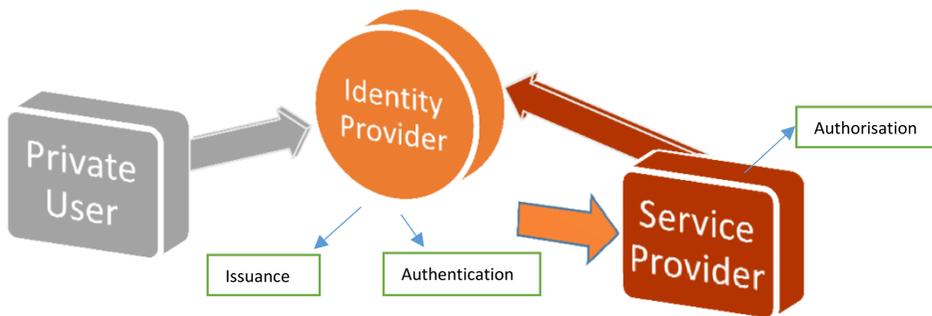


Figure 2. Centralized identity management system.

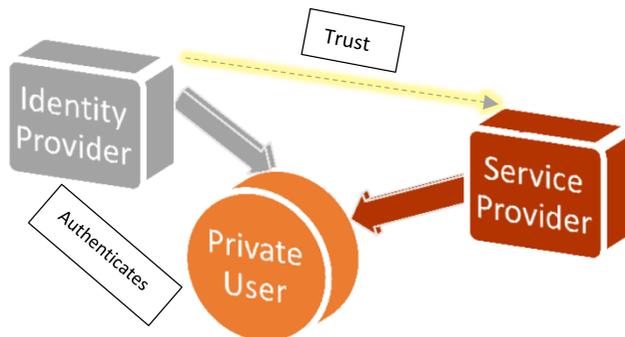


Figure 3. Federated identity systems.

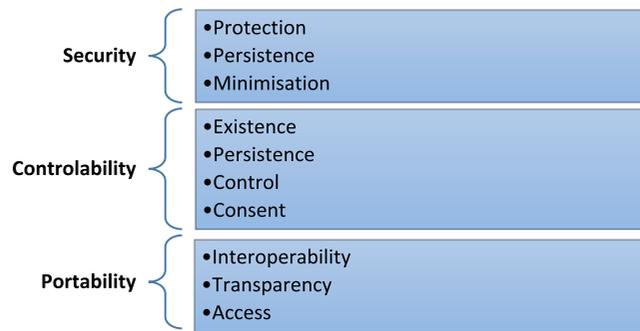


Figure 4. Self-sovereign identity principles inspired by [Tobin and Reed \(2017\)](#).

to store and share data, the user controls the data and can decide with whom to share which data. [Swan \(2017, p. 7\)](#) argued that “centralized databases provide an attractive target for hackers, whereas it is possible that decentralized storage records protected by cryptographic signatures on blockchains might dramatically improve network cybersecurity.”

Initially used for decentralized cryptocurrencies such as Bitcoin, blockchain has been successfully adopted in various domains for different types of information sharing. Its basic concept is that transactions are secure, transparent, and immutable within a chain of records stored in data blocks in a decentralized network. The chain of transactions is duplicated by each additional block developing a distributed ledger system ([Nofer et al., 2017](#)). The system is operated in a peer-to-peer model that does not need a third party to transact. As such, blockchain-based SSI is based on distributed consensus and trust mechanisms in an environment of collaboration.

Blockchain technology can bring new options to the data storage for identification and, therefore, change the relationship between the actors involved. This includes “moving away from intermediary and provider-controlled identity management models towards user-controlled digital identity” ([Aydar & Ayvaz, 2019, p. 2](#)).

Immutable identities based on blockchain platforms could be a game-changer for world poverty ([Thomason et al., 2018](#)) to promote social-economic ([Wang & De Filippi, 2020](#)) and global financial inclusion ([Swan, 2017](#)), support access to healthcare and secure patient’s health information (eHealth), and support effective humanitarian response. In this context, SSIs can accelerate inclusive development and “increase the accuracy and reliability of identity data and credentials” ([World Bank Group, 2021](#)).

DLT is the term used to describe a decentralized database infrastructure that allows the distribution of information in an immutable ledger of a group of users of a smart network ([Bouras et al., 2020](#)). In these secured ledgers, individuals can store their personal information without the involvement of any third party ([Bernal Bernabe et al., 2019](#); [Bouras et al., 2020](#)). Blockchain technology is a type of DLT that supports the viability of SSIs.

[Tobin and Reed \(2017\)](#) claim that the best way to understand SSIs is to consider them as a “digital record or container of identity” controlled by the user. In another attempt to conceptualize SSI, [Giannopoulou \(2020, p. 2\)](#) describes it “as an identity management system, developed by a private or public entity which takes technological design decisions for personal data management guided by a set of principles that are loosely defined and not universally accepted as a common standard.” These principles were proposed by [Allen \(2016\)](#) and are grouped into three main areas, namely: security, controllability, and portability, and confirm that the user remains the one managing their data [Figure 4](#).

Due to the novelty of this technology, there is no common understanding of its structure; nevertheless, some essential attributes can be listed:

- User-centric
- Consent
- Immutability
- Trust
- Privacy

Table 1. Evolution of identity management systems (IdMs) and the innovation brought by self-sovereign identities (SSIs; inspired by Sensors, 2020).

Characteristics	Centralized IdMs	Federated IdMs	Blockchain-based SSI
User control/Autonomy	–	–	
Privacy	Risky	Risky	
Consent	–	–	
Immutability	–	–	
Trust (smart network)	–	–	

Unlike centralized and federated IdMs where the service provider was at the heart of the identity model, SSI is user-centric, and the blockchain architecture replaces the registration authority from classic IdM designs (Mühle et al., 2018). This user-centric aspect removes the external control (third party intermediation), enabling the individual or organization the full ownership, control, and management of their identity (Tobin & Reed, 2017). Consequently, the SSI transfers to the user the complete governing of their identity credentials and the decision to whom and to which extent their personal data will be disclosed.

SSIs' consent, immutability, and trust attributes derive from the main pillars of blockchain. Blockchain uses the millennial art of cryptography to provoke its disruptive impact through distributed ledgers in which an immutable and unique digital fingerprint—the hash—is recorded (Iansiti & Lakhani, 2017), distributed, verified, and monitored by multiple sources simultaneously (consensus).

In terms of privacy, SSI design innovates by providing a high level of data security due to its “privacy-preserving solutions” on “crypto-privacy techniques” (Bernal Bernabe et al., 2019). Based on the SSI principles, it is possible to determine that privacy issues relate to an immutable identity's security (protection/confidentiality) and controllability (control). Danezis and Gürses (2010) clarify that the notion of confidentiality stands for “either minimizing the collected information, anonymizing the collected information, or securing the collected information from unauthorized access,” while the ability to control how your data are shared is also a benefit covered by the privacy design of SSIs Table 1.

Blockchain-based SSIs reduce the need for intermediaries, and as the technology further matures, it can lead to “a structural shift of power from legal rules and regulations administered by government authorities to code-based rules and protocols governed by decentralized blockchain-based networks” (De Filippi & Wright, 2018). While the technology begins to be adopted in diverse domains, it is expected that concerns will raise. Jun (2018, p. 201) states that different from the Internet where each State controls a cross-border environment, “blockchain is based on the P2P structure and has a technical basis that precludes effective state control.” This effect by itself disrupts the traditional concept of State power we have known and accepted up until these days. The conventional geographical borders do not bound online interactions. The technology, however, needs to mature to deliver all its promises as a digital identity solution (Van Bokkem et al., 2019).

Whereas in traditional IdM systems organizations are the stewards of the user data, SSIs enable users to fully control their information and bring a paradigm shift in personal data storage. Through an SSI blockchain-based application, individuals are able to create an encrypted identity and govern their data; moreover, a digital ID can be generated and used as a verified stamp in online transactions (Monrat et al., 2019). These characteristics combined with blockchain-based platforms' unique environment disrupt the known personal data governance models, as blockchain technologies provide a data governance platform by definition.

Identity perspectives

Identity is a concept that has various connotations and is not uniform. Individuals in their social interactions share particular roles, belong to specific groups, and identify themselves through personal attributes that make them unique (Stets & Burke, 2010) and as a result, demand recognizing their identity through diverse ways, based on religion, politics, gender, economics, and other social approaches. Klandermans (2014) argued that people engage in various societal roles and therefore hold multiple identities, in what he calls “simultaneous existence of various identities” (p. 11).

Fukuyama (2018) stated that until the social movements of the second half of the 20th century, the concerns about identity were connected to individual capabilities, in opposition to the questions related to social groups. In this historical moment, explains the author, the rise of modern democracy culminated with the acceptance that individuals are equal in their essence but still not similarly respected as marginalized groups still struggle for the adequate recognition of their identity and their social worth.

In this context, the discussion about identity politics becomes valuable for social sciences as an attempt to acknowledge the experience of injustices of certain social groups (Heyes, 2020) and the respect of social and cultural pluralism deriving from various group identities with the goal of self-determination (Heyes, 2002). As a consequence, Fukuyama (2018) argued that the “desire for equal recognition can easily slide over into a demand for recognition of the group’s superiority. This is a large part of the story of nationalism and national identity, as well as certain forms of extremist religious politics today.” Hence, the notion of identity politics is so crucial for changes in public policies and the mitigation of injustices. At the same time, “often governments fail to secure equality in society or deliberately establish and maintain inequality” (Klandermands, 2014). From a social perspective, identity politics can encompass religious identities, economic identity, national identity, gender identity, and the demand for inclusiveness.

From a legal angle, Wang and De Filippi (2020) state that identity is related to the definition of a “natural” and “legal” person, which implies the condition of being a citizen and the legal ability to exercise rights and duties. This legal recognition is a fundamental human right (Thomason et al., 2018), grants individuals access to essential services, and is taken for granted in countries with efficient registration systems (Vandenabeele & Lao, 2007). For inclusion, having an identity is essential, as identity is required to be able to transact with the government. Yet, sometimes people might want to be anonymous.

Although the right to be recognized before the law is established in the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights, according to the World Bank Group (2018), in 2018, more than 1 billion people still lack official proof of their identity. The majority of them are women and the poor living in low-income countries and underserved communities. Being socially invisible and having no means to prove who they are, these individuals are denied the right to access essential public services, to be able to be supported by financial aid, to pursue proper education, to be able to apply for a formal job, to participate in the democratic debate, among other limitations within social, political, and civil life. Moreover, being “invisible” also highlights their vulnerability to abuses and degrading treatment. The importance of the identification is so crucial that the SDG-UN includes the provision of legal identity for all by 2030 (SDG Goal 16.9). The adoption of SSIs can serve as an economic inclusion tool and, consequently, a powerful instrument in public value creation through the relationship between the public sector and the citizens (Jørgensen & Bozeman, 2007). However, this requires changes in the institutional context of IdMs.

In conclusion, what constitutes identity and who should issue it are essential considerations. In addition to the identity-related issues, there are policy and governance challenges to overcome.

Policy and governance challenges on the adoption of SSI

The adoption of SSIs also brings policy and governance challenges, including the role of the government, the control of the data, the governance of the SSI development and maintenance, and for which purposes, the SSI can be used.

As an instrument for better governance, Thomason et al. (2018 p. 3) argued that SSIs core characteristics of immutability and user-centric “assist in the mitigation of legitimate privacy concerns that developed nations currently face in existing state-based, digital identity programs.” Atzori (2017) stated that blockchain can be viewed as a technology that competes with the role of government in society. The SSI enables users to share their data without the need for governments to operate registries.

Blockchain technology enables that instead of transactions being handled directly by government organizations, they can be operated by DLT. This is called *governance by blockchain*. On the other hand, the SSI software needs to be initiated and maintained. The various nodes of the distributed ledger need to be operated. Access to the ledger can be restricted, and the number of nodes and the type of consensus mechanism needs to be determined. This is called *governance of SSI technology or SSI governance*.

The party that sets up the SSI governance defines the game’s rules and determines how changes in the future will be handled. A public or private entity, namely governments, notaries, or tech companies, can play this role. Independent of who is setting up the SSI, regulations are needed to establish the

legal framework and provide clarity and legal security. Legislation should prevent misuse and ensure the creation of public values, like privacy and transparency, and should determine the status of the SSI. For example, what value is contributed to the data in the SSI, and for what purposes can the data in the SSI be trusted.

Regulatory functions consist of three main groups: (1) the architecture design; (2) establishing rules governing; and (3) the interactions between users (Di Porto & Zuppeta, 2021). In blockchain-based SSI, architecture design and governing rules are related, as the latter are embedded in the design. Government regulations determine the legal status of the use of SSI. For example, the SSI purpose to be used within a specific jurisdiction, the possibility of use in the public and private sectors, and how to deal with different SSIs should be answered by regulations. In addition, more SSI applications might eventually emerge, and how they will be operated, maintained, and accepted in various jurisdictions needs to be answered.

Governance is also needed to deal with issues like identity theft, fraud, or misuse of the data. Once a villain party takes over someone's identity, the government should have the ability to interfere and remove or reset the SSI. This requires some level of control from the government. Furthermore, users might not be able to change essential information without previous checks. For this purpose, consensus mechanisms need to be introduced in which both government(s) and users have to agree before any data modification is performed, like address data or property.

When governments implement and adopt SSI, the outcomes vary. Fountain's (2001) TEF can be used to explain the impact of technology by investigating the organizational structure and institutional arrangements. This TEF can be used to describe how organizational and institutional variables affect the perception of and the selection, implementation, and use of blockchain-based SSI. The enactment process is nonlinear and allows individuals to adapt information technologies to existing organizational routines, work practices, and individual relationships (Luna-Reyes et al., 2016). Through the enactment process, stakeholders select the features of certain objective technologies, which are affected by organizational characteristics and institutional arrangements. This results in the stakeholders enacting technologies that reinforce the current status and power structures (Fountain, 2001; Kraemer & King, 1986). From the government stakeholder perspective, SSI is presented to address the control and data quality problems in public administration, which should be enacted. The SSI literature suggests a shift from data control from the government to the citizens (Mühle et al., 2018). In the Netherlands, also politicians embrace this point of view, as shown by arrow (1) in the figure below.

The TEF suggests that both bureaucratic structure and the behavior of key stakeholders will determine technology enactment and outcomes. Kraemer and King (1986) found that digitalization can only be understood by understanding the forces that shape organizational decision-makers' ideas. Stakeholders' perceptions enact the technology, which is influenced by existing institutional arrangements. Mental habits and cognitive models that influence behavior and decision-making like the risk-averse culture of the government and the desire to control the data quality can result in governments' strengthening in controlling the data, instead of a shift toward more control by the citizens. This is shown by (2) in Figure 5. Citizens might merely function as an input medium for updating their data that need to be approved by the government, which is responsible for the data quality, preventing the possible misuse of data for fraud. Therefore, a high level of control is exercised by the government.

Yet, governments should also consider using SSI technology as a tool for inclusion and a more balanced view on control is needed. Inclusion by SSIs could embrace those marginalized and who live

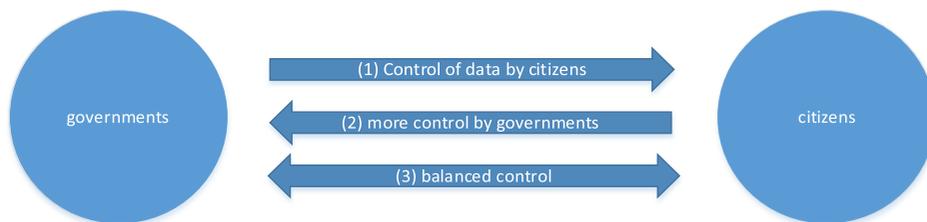


Figure 5. The shift in the power balance.

under social or digital exclusion (Jaeger et al., 2012), as the undocumented immigrants (Benchaya Gans et al., 2020), vulnerable consumers (Clifton et al., 2019), and, therefore, promoting social-economic growth and human development (Addo & Senyo, 2021).

Furthermore, an essential characteristic of information exchange is the promotion of transparency. Hence, governments (as institutions) should generally not be allowed to operate in secrecy and should ensure that their decisions and actions are transparent and auditable (Janssen & van den Hoven, 2016). In particular, when information is altered or used should be visible to citizens. This can be accomplished by adhering to the principle of information-based transparency, e.g., when data are shared information about a person or an organization, these entities should be informed (Janssen et al., 2020). This avoids misuse of the identity, and possible misuse and theft can be immediately detected.

Governments might easily enact the SSI technology by making only visible what they aim to show, but not the actual use of data to inspect corruption detection, for instance. A more balanced view should be found in which citizens are also given some control. This is a more balanced approach, as shown by arrow (3) in Figure 5. There is a need for more research on how this balance can be found.

Conclusions

Identity information is very sensitive and should be strictly governed. SSI has the potential to transform the relationship between governments, companies, and users. The introduction of SSI requires significant changes in various aspects related to governance decisions and data control, aiming the prevention and solving of fraud and misuses, the organization in charge of the SSI development and maintenance, regulation for legitimacy and realizing public values, and for which purposes, the SSI can be used. These decisions will shape and influence the societal impact.

Citizens and governments have a relationship in which the government is traditionally powerful. SSI can strengthen the role of citizens and their power but also weaken its positions. SSI literature often takes a simplistic view of societal implications by focussing on empowering users. The technology enactments theory suggests that the SSI will be influenced by the existing bureaucratic structure and the behavior of key actors, and the current power structure will be enacted. The latter might only reinforce current practices and provide no better user control or improved privacy. A more balanced approach is when transparency and clear governance are introduced for identity data changes in which both users and governments are involved. Also, holding multiple identities should be possible, as humans have different roles in society.

Further research should investigate how SSIs can be designed and governed to ensure a proper balance between citizen and government control so that public values like transparency and privacy are guaranteed, and fraud and corruption are avoided. In addition, the concept of identity should be further unraveled to steer the design of SSI.

Funding

This research was supported by the Erasmus+ Programme of the European Union, project reference number 598273-EPP-1- 2018-1-ATEPPKA2-CBHE-JP.

Conflict of interest

None declared.

References

- Addo, A., & Senyo, P. K. (2021). Advancing E-governance for development: Digital identification and its link to socioeconomic inclusion. *Government Information Quarterly*, 38(02), 101568. <https://doi.org/10.1016/j.giq.2021.101568>.
- Allen, C. (2016). *The path to self-sovereign identity*. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.
- Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, 6(01), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5.
- Aydar, M., & Ayvaz, S. (2019). Towards a Blockchain-based digital identity verification, record attestation and record sharing system. *ArXiv*, abs/1906.09791.

- Benchaya Gans, R., Ubacht, J., & Janssen, M. (2020). Self-sovereign identities for fighting the impact of COVID-19 Pandemic. *Digital Government: Research and Practice*, 2, 2. Article 16, 4 pages. <https://doi.org/tudelft.idm.oclc.org/10.1145/3429629>.
- Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908–164940. <https://doi.org/10.1109/ACCESS.2019.2950872>.
- Birrell, E., & Schneider, F. B. (2013). Federated identity management systems: A privacy-based characterization. *IEEE Security & Privacy*, 11(05), 36–48. <https://doi.org/10.1109/MSP.2013.114>.
- Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., Zhang, T., & Ning, H. (2020). Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors (Switzerland)*, 20(02), 1–20.
- Chadwick, D. W. (2013). Federated identity management systems. *IEEE Security and Privacy*, 11(5), 36–48.
- Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, 37(02), 205–219. [https://doi.org/10.1016/S1389-1286\(01\)00217-1](https://doi.org/10.1016/S1389-1286(01)00217-1).
- Clifton, J., Díaz-Fuentes, D., & Fernández-Gutiérrez, M. (2019). Vulnerable consumers and satisfaction with public services: Does country matter? *International Review of Administrative Sciences*, 85(02), 264–285. <https://doi.org/10.1177/0020852317691341>.
- Danezis, G., & Gürses, S. (2010). A critical review of 10 years of Privacy Technology. *Proceedings of Surveillance Cultures: A Global Surveillance Society*, 1–16.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press. <https://doi.org/10.2307/j.ctv2867sp>.
- Dhamija, R., & Dussault, L. (2008). The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy*, 6(02), 24–29. <https://doi.org/10.1109/MSP.2008.49>.
- Di Porto, F., & Zuppetta, M. (2021). Co-regulating algorithmic disclosure for digital platforms. *Policy and Society*, 40(02), 272–293. <https://doi.org/10.1080/14494035.2020.1809052>.
- Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security & Privacy*, 16(04), 20–29. <https://doi.org/10.1109/MSP.2018.3111247>.
- Fountain, J. E. (2001). *Building the virtual state: Information technology and institutional change*. Brookings Institution Press.
- Fukuyama, F. (2018). *Identity: The demand for dignity and the politics of resentment*. Kindle Edition.
- Giannopoulou, A. (2020). Data protection compliance challenges for self-sovereign identity. *Advances in Intelligent Systems and Computing*, vol 1238 Springer, Cham. https://doi.org/tudelft.idm.oclc.org/10.1007/978-3-030-52535-4_10.
- Gilani, K., Bertin, E., Hatin, J., & Crespi, N. (2020). A survey on blockchain-based identity management and decentralized privacy for personal data. 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) pp. 97–101. <https://doi.org/10.1109/BRAINS49436.2020.9223312>.
- Heyes, C. (2020). Identity politics. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. <http://plato.stanford.edu/tudelft.idm.oclc.org/archives/fall2002/entries/identity-politics/>.
- Heyes, C. (2002). Identity politics. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Fall 2002 edition. Electronic document: <http://plato.stanford.edu/tudelft.idm.oclc.org/archives/fall2002/entries/identity-politics/>.
- Iansiti, M., & Lakhani, R. K. (2017). The Truth about Blockchain - It will take years to transform business, but the journey begins now. *Harvard Business Review*, Jan-Feb. <https://hbr.org/2017/01/the-truth-about-blockchain>.
- Jaeger, P. T., Bertot, J. C., Thompson, K. M., Katz, S. M., & DeCoster, E. J. (2012). The intersection of public policy and public access: Digital divides, digital literacy, digital inclusion, and public libraries. *Public Library Quarterly*, 31(01), 1–20. <https://doi.org/10.1080/01616846.2012.654728>.
- Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, 37(03), 101493. <https://doi.org/10.1016/j.giq.2020.101493>.
- Janssen, M., & van den Hoven, J. (2016). Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy? *Government Information Quarterly*, 32(04), 363–369. <https://doi.org/10.1016/j.giq.2015.11.007>.
- Jørgensen, T. B., & Bozeman, B. (2007). Public values: An inventory. *Administration & Society*, 39(03), 354–381. <https://doi.org/10.1177/0095399707300703>.

- Jun, M. (2018). Blockchain government - a next form of infrastructure for the twenty-first century. *Journal of Open Innovation: Technology, Market, and Complexity*, 4(1). MDPI AG. <http://dx.doi.org/10.1186/s40852-018-0086-3>.
- Klandermands, P. G. (2014). Identity politics and politicized identities: Identity processes and the dynamics of protest. *Political Psychology*, 35(01), 1–22. International Society of Politica. <https://doi.org/10.1111/pops.12167>.
- Kraemer, K. L., & King, J. L. (1986). Computing and public organizations. *Public Administration Review*, 46(03), 488–496. <https://doi.org/10.2307/975570>.
- Lips, M. (2006). E-government under construction: Challenging traditional conceptions of citizenship. In P.G. Nixon, V.N. Koutrakou (Eds.), *E-Government in Europe: Re-booting the state* (pp. 33–47). (1st ed.), Routledge. <https://doi.org/10.4324/9780203962381>.
- Luna-Reyes, L. F., Picazo-Vela, S., Luna, D. E., & Gil-Garcia, J. R. (2016). Creating public value through digital government: Lessons on inter-organizational collaboration and information technologies. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS) (HICSS' 16) (pp. 2840–2849). IEEE Computer Society, USA, 2840–2849. <https://doi-org.tudelft.idm.oclc.org/10.1109/HICSS.2016.356>.
- Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7, 117134–117151. <https://doi.org/10.1109/ACCESS.2019.2936094>.
- Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80–86. <https://doi.org/10.1016/j.cosrev.2018.10.002>.
- Naik, N., & Jenkins, P. (2020). Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology. In Proceedings - 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 90–95. IEEE. <https://doi.org/10.1109/MobileCloud48802.2020.00021>.
- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business and Information Systems Engineering*, 59(03), 183–187. <https://doi.org/10.1007/s12599-017-0467-3>.
- Shim, S. S. Y., Bhalla, G., & Pendyala, V. (2005). Federated identity management. *Computer*, 38(012), 120–122. <https://doi.org/10.1109/MC.2005.408>.
- Stets, J. E., & Burke, P. J. (2010). Identity theory and social identity theory. *Social Psychology Quarterly*, 63(03), 224–237. <https://doi.org/10.2307/2695870>.
- Stryker, S., & Burke, P. J. (2010). The past, present, and future of an identity theory. *Social Psychology Quarterly*, 63(04), 284–297. <https://doi.org/10.2307/2695840>.
- Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology Innovation Management Review*, 7(010), 6–13. <https://doi.org/10.22215/timreview/1107>.
- Thomason, J., Ahmad, M., Bronder, P., Hoyt, E., Pocock, S., Bouteloupe, J., Donaghy, K., Huysman, D., Willenberg, T., Joakim, B., Joseph, L., Martin, D., & Shrier, D. (2018). Blockchain-powering and empowering the poor in developing countries. In A. Marke (ed.), *Transforming climate finance and green investment with blockchains* (pp. 137–152). Academic Press. <https://doi.org/10.1016/B978-0-12-814447-3.00010-0>.
- Tobin, A., & Reed, D. (2017). *The inevitable rise of self-sovereign identity*. White Paper, 29 (September 2016), 10. <https://sovrin.org/library/>.
- Ulicane, I., Knight, W., Leach, T., Stahl, B. C., & Wanjiku, W. G. (2020). Framing governance for a contested emerging technology: Insights from AI policy. *Policy and Society*, 40(02), 158–177. <https://doi.org/10.1080/14494035.2020.1855800>.
- Van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (2019). Self-sovereign identity solutions: The necessity of blockchain technology. *arXiv*. preprint arXiv:1904.12816.
- Vandenabeele, C., & Lao, C. V. (2007). *Legal identity for inclusive development*. Asian Development Bank. <http://hdl.handle.net/11540/4860>.
- 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*, 2. <https://doi.org/10.3389/fbloc.2019.00028>.
- Wang, K., Dong, J., Wang, Y., & Yin, H. (2019). Securing data with blockchain and AI. *IEEE Access*, 7, 77981–77989.
- World Bank Group. (2018). *Global ID4D database (English)*. <https://datacatalog.worldbank.org/dataset/identification-development-global-dataset>.

- World Bank Group. (2021). *Principles on identification for sustainable development: Toward the digital age - second Edition (English)* <http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age-Second-Edition>.
- Xu, J., Xue, K., Tian, H., Hong, J., Wei, D. S. L., & Hong, P. (2020). An identity management and authentication scheme based on redactable blockchain for mobile networks. *IEEE Transactions on Vehicular Technology*, 69(06), 6688–6698. <https://doi.org/10.1109/TVT.2020.2986041>.