12-12-2021

Self-sovereign identity: a primer and call for research in information systems

Jacob Young
Bradley University, jayoung@bradley.edu

Sahar Farshadkhah
University of Illinois Springfield

Self-Sovereign Identity: A Primer and Call for Research in Information Systems

Jacob A. Young[1]
Foster College of Business, Bradley University,
Peoria, Illinois, United States

Sahar Farshadkhah
College of Business and Management, University of Illinois Springfield,
Springfield, Illinois, United States

ABSTRACT

In this research-in-progress paper, we encourage information systems (IS) researchers to consider the self-sovereign identity (SSI) approach to identity management. We highlight several issues with current data practices, then provide an overview of SSI by discussing the technology and actors involved. Finally, we call for more IS research on SSI to ultimately increase its adoption.

Keywords: self-sovereign identity, identity management, privacy, security.

INTRODUCTION

Every person provides data to every organization with which they interact without oversight or control from the original owner of the data (James et al. 2017). This lack of control often leads to organization information overreach (Graeff and Harmon 2002), data loss (Lesnykh 2011), and ultimately destructive behavior (Samtani et al. 2017). To address these issues, we encourage information systems (IS) researchers to consider self-sovereign identity (SSI).

SSI is user centric and promises to be trustworthy, private, and secure (Mühle et al. 2018). Under SSI, users completely own and control their digital data. This affords the ability to selectively share data with third parties without relying on a trusted custodian. Before advocating for SSI, we begin by highlighting several issues with current data practices, such as the

[1] Corresponding author. jayoung@bradley.edu +1 309 677 3718

implications for user security, privacy, and liberty. We then provide an overview of SSI by discussing the technology and actors involved. Finally, we call for more IS research on SSI to ultimately increase its adoption.

BACKGROUND

Secondary information use, where personal information is "used for other purposes subsequent to the original transaction between an individual and an organization when the information was collected," has been a concern for decades (Culnan 1993). However, the birth of the Internet and the rapid proliferation of ubiquitous Internet-connected devices enhanced the ability for data brokers and criminals to collect, distribute, and publish highly sensitive personal information about others without their explicit knowledge or consent (Anthes 2015). These technology advancements have only exacerbated the growing threat to an individual's security, privacy, and liberty.

Security

Early research suggested that security breaches can negatively impact a firm's stock price (Gatzlaff and McCullough 2010), yet several studies have failed to find significant effects, which could possibly be attributed to investors becoming numb to breaches (Foecking et al. 2021; Frimpong and Chen 2021; Makridis 2021; Richardson et al. 2019). U.S. courts also hold that victims do not have standing to sue for future damages that may result from a breach (Steffel 2019). Even worse, victims of identity theft rarely receive any meaningful compensation, especially when data breaches often result in permanent and irreparable damage.

Although news of data breaches and leaks litter the headlines, too little effort has been made to curtail the "collect it all" approach that largely resulted from the rise of big data analytics (Gonsowski 2020). Ideally, firms would adhere to the "don't collect what you can't

protect" principle by implementing data minimization strategies (Bejtlich 2015). Unfortunately, the perceived value and supposed insights that can be gleaned from massive data repositories, coupled with the lack of financial consequences, further reduces a firm's motivation to improve their data collection and security practices.

Privacy

New technology, such as wearable devices (Banerjee et al. 2018), biometrics (Royakkers et al. 2018), and voice assistants (Barrett and Liccardi 2021), has dramatically increased privacy risks by generating, storing, and transmitting troves of highly sensitive information. Therefore, users must put their faith in system developers and trust that the privacy protections and settings will perform as advertised (Fowler and Hunter 2021; Lin and Halloran 2021).

Although there have been numerous calls for reform, such as enhancing privacy policies (Culnan 2019), the U.S. has yet to pass comprehensive data privacy and security legislation. Until a federal law is passed (e.g., the European Union's General Data Protection Regulation's (GDPR) (Politou et al. 2018)), data protection laws are limited to specific economic sectors (Smith 2020). Although some states have enacted their own data privacy laws, such as California's Consumer Protection Act (Ghelardi 2021) and the Illinois Biometric Information Privacy Act (Stepney 2019), it is important to note that the increasing affordability and ubiquitous nature of more capable devices will make it difficult to enforce any well-intentioned legislation across all of society without focusing on the data collection itself.

Liberty

While George Orwell's fear of a totalitarian government becoming "Big Brother" was initially kept in check by the cost of deploying the necessary technology, the increasing value of personal information has resulted in the rise of "surveillance capitalism," where the insatiable

appetite for data has justified immense private-sector investment in collection and monitoring capabilities (Power 2016; Zuboff 2015). Thanks to the third-party doctrine, governments now have a nearly unfettered access to troves of sensitive data held by other organizations, which can lead to significant abuses (Thompson 2014). Governmental responses to certain events, such as the terror attacks of September 11, 2021 (Solove 2007), and the COVID-19 pandemic (Brough and Martin 2021), highlight how just how quickly modern technology can be employed to surveil, discriminate against, and control the behavior of various segments of society.

While updated legislation might curb some behaviors and provide victims with more reasonable compensation, the inability to ensure that sensitive information entrusted to others can be adequately protected will remain a fatal flaw with respect to current data practices. Therefore, we encourage organizations to consider adopting the SSI approach to data collection and identity management.

SELF-SOVEREIGN IDENTITY

Ferdous et al. (2019) organized the essential properties of SSI into five categories: (1) foundational, (2) security, (3) controllability, (4) flexibility, and (5) sustainability. Foundational properties define the SSI context, such as existence, autonomy, ownership, access, and single source. Protection, availability, and persistence guarantee the security of SSI. Controllability properties consist of choosability, disclosure, and consent. Flexibility properties ensure that SSI is flexible enough to work with different systems, such as portability, interoperability, and minimization. Transparency, standard, and cost are referred to as sustainability properties. Blockchain technology can satisfy several properties of SSI, such as availability, access, and disclosure.

Table 1. Self-Sovereign Identity Properties

Category	**Properties**
Foundational	existence, autonomy, ownership, access, and single source
Security	protection, availability, and persistence
Controllability	choosability, disclosure, and consent
Flexibility	portability, interoperability, and minimization
Sustainability	transparency, standard, and cost

Given SSI's simplicity, there is a seemingly infinite number of use cases where SSI could be considered. For example, if an individual needed to prove his or her employment status to qualify for a loan, the employer would be the issuer, the holder would be the employee, and the verifier would be the bank who is requesting the information.

Distributed Ledger Technology & Blockchain

Distributed Ledger Technology (DLT), as one of the most promising innovations in the field of information technology, is the core of blockchain. Even though the terms blockchain and DLT are used interchangeably in the literature, there is a subtle difference between them. A blockchain is "a DLT concept comprising a chain of cryptographically linked, chronologically ordered, 'blocks' containing batched transactions" (Sunyaev 2020, p. 285). Blockchains have several specifications that makes it a proper candidate for SSI. Blockchains satisfy the availability and accessibility properties of SSI by providing a decentralized domain that makes data readily available to any authorized entity. Since the owner has full control of sharing data with others, blockchain technology also satisfies the disclosure property. Ferdous et al. (2019) also argues that blockchain technology outperforms traditional approaches when it comes to data immutability, provenance, distributed control, accountability, and transparency.

Actors

SSI solutions involve three different actors: issuer, holder, and verifier. An issuer is an entity who issues credentials after verifying claims about a subject, such as a bank, the

Department of Motor Vehicles (DMV), or an employer. A verifier is an entity that requests and verifies the credentials. A holder is usually, but not always, a subject of the credentials. Holders request and obtain credentials from the issuer, which can then be presented to others to satisfy various requirements. The verifier can authenticate credentials by checking the blockchain to verify that the claim has been digitally signed by a trusted issuer. We illustrate the relationship among each actor and the blockchain in Figure 1.

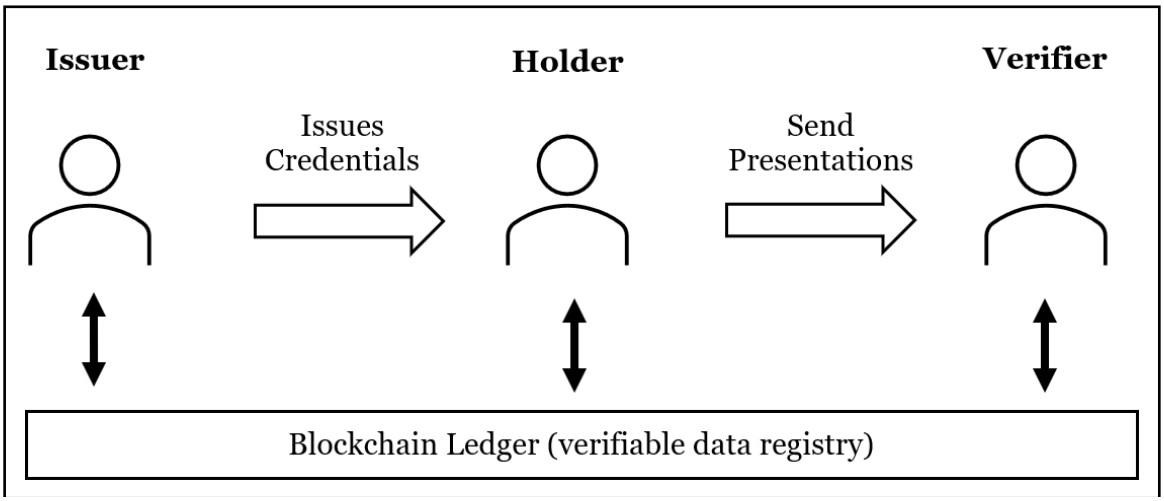

Figure 1. Self-Sovereign Identity Actors

Verifiable Credentials and Zero-Knowledge Proofs

A verifiable credential is a set of one or more claims which might also include metadata about the issuer (W3C 2019). Since the binary data stored on the blockchain only pertains to the validity of the claim, not the underlying data, it holds no value to identity thieves. A zero-knowledge proof (ZKP) is a cryptographic technique that ultimately makes the SSI approach possible. ZKPs give the holder the ability to convince a verifier that the claim presented in the credential is true, all without disclosing any additional information (Yang and Li 2020). For example, using a ZKP, the holder can share the credential that shows "AGE > 18 = TRUE," which was issued by the State Department of Motor Vehicles, without revealing any underlying

information like his or her date of birth. Using a ZKP, a holder even can combine multiple verifiable claims from different issuers and share it in a single verifiable presentation without leaking any extra information. Moreover, the ZKP method provides flexibility for holders to use their issued verifiable credentials in any context that they desire (W3C 2019).

DISCUSSION

In this paper, we provided an overview of SSI and highlighted several advantages. Although SSI has been briefly mentioned in a few IS research streams, such as artificial intelligence (Janssen et al. 2020), big data (Young, Smith, et al. 2020), cybersecurity (Gal and McCarthy 2018), privacy (Bernabe et al. 2019; Sunda 2020; Young, Biros, et al. 2020), identity management (Gal and McCarthy 2018; Ishmaev 2020; Laatikainen, Kolehmainen, and Abrahamsson 2021; Laatikainen, Kolehmainen, Li, et al. 2021), healthcare (Hasan et al. 2020; Houtan et al. 2020; Ishmaev et al. 2021) and whistleblowing (Young and Farshadkhah 2021), we believe that deeper research should be conducted in various contexts to strengthen the argument for wider adoption of SSI. We hope that our primer will foster increased attention on innovative identity management solutions, such as SSI, in future IS research.

REFERENCES

Anthes, G. 2015. "Data Brokers Are Watching You," *Communications of the ACM* (58:1), pp. 28–30. (https://doi.org/10.1145/2686740).

Banerjee, S. (Sy), Hemphill, T., and Longstreet, P. 2018. "Wearable Devices and Healthcare: Data Sharing and Privacy," *The Information Society* (34:1), Taylor & Francis, pp. 49–57. (https://doi.org/10.1080/01972243.2017.1391912).

Barrett, L., and Liccardi, I. 2021. "Accidental Wiretaps: The Implications of False Positives By Always-Listening Devices For Privacy Law & Policy." (https://doi.org/10.2139/ssrn.3781867).

Bejtlich, R. 2015. "New Cybersecurity Mantra: 'If You Can't Protect It, Don't Collect It,'" *Brookings Institution*. (https://www.brookings.edu/blog/techtank/2015/09/03/new-cybersecurity-mantra-if-you-cant-protect-it-dont-collect-it/).

Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., and Skarmeta, A. 2019. "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access* (7),

IEEE, pp. 164908–164940. (https://doi.org/10.1109/ACCESS.2019.2950872).
Brough, A. R., and Martin, K. D. 2021. "Consumer Privacy During (and After) the COVID-19 Pandemic," *Journal of Public Policy & Marketing* (40:1), pp. 108–110. (https://doi.org/10.1177/0743915620929999).
Culnan, M. J. 1993. "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly* (September), pp. 341–363.
Culnan, M. J. 2019. "Policy to Avoid a Privacy Disaster," *Journal of the Association for Information Systems* (20:6), pp. 848–856. (https://doi.org/10.17705/1jais.00554).
Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. 2019. "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," *IEEE Access* (7), pp. 103059–103079. (https://doi.org/10.1109/ACCESS.2019.2931173).
Foecking, N., Wang, M., and Huynh, T. L. D. 2021. "How Do Investors React to the Data Breaches News? Empirical Evidence from Facebook Inc. during the Years 2016–2019," *Technology in Society* (67:March), Elsevier Ltd, p. 101717. (https://doi.org/10.1016/j.techsoc.2021.101717).
Fowler, G. A., and Hunter, T. 2021. "When You 'Ask App Not to Track,' Some IPhone Apps Keep Snooping Anyway," *The Washington Post*, , September 23. (https://www.washingtonpost.com/technology/2021/09/23/iphone-tracking/).
Frimpong, B., and Chen, L. 2021. "The Effects of Data Breaches on Public Companies: A Mirage or Reality?," *Advances in Intelligent Systems and Computing* (1363 AISC), pp. 674–683. (https://doi.org/10.1007/978-3-030-73100-7_49).
Gal, G., and McCarthy, W. E. 2018. "Can Blockchains and REA Smart Contracts Address Certain Cybersecurity Issues," *2018 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, (A. Vance, ed.), pp. 1–24.
Gatzlaff, K. M., and McCullough, K. A. 2010. "The Effect of Data Breaches on Shareholder Wealth," *Risk Management and Insurance Review* (13:1), pp. 61–83. (https://doi.org/10.1111/j.1540-6296.2010.01178.x).
Ghelardi, E.-M. 2021. "Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act," *St. John's Law Review* (94:3), pp. 869–893.
Gonsowski, D. 2020. "Protecting Privacy by Minimizing Data," *Risk Management* (67:6), pp. 12–14.
Graeff, T. R., and Harmon, S. 2002. "Collecting and Using Personal Data: Consumers' Awareness and Concerns," *Journal of Consumer Marketing* (19:4), pp. 302–318. (https://doi.org/10.1108/07363760210433627).
Hasan, H. R., Salah, K., Jayaraman, R., Arshad, J., Yaqoob, I., Omar, M., and Ellahham, S. 2020. "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," *IEEE Access* (8), pp. 222093–222108. (https://doi.org/10.1109/ACCESS.2020.3043350).
Houtan, B., Hafid, A. S., and Makrakis, D. 2020. "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare," *IEEE Access* (8), pp. 90478–90494. (https://doi.org/10.1109/ACCESS.2020.2994090).
Ishmaev, G. 2020. "Sovereignty, Privacy, and Ethics in Blockchain-Based Identity Management Systems," *Ethics and Information Technology* (0123456789), Springer Netherlands.

(https://doi.org/10.1007/s10676-020-09563-x).

Ishmaev, G., Dennis, M., and van den Hoven, M. J. 2021. "Ethics in the COVID-19 Pandemic: Myths, False Dilemmas, and Moral Overload," *Ethics and Information Technology* (0123456789), Springer Netherlands. (https://doi.org/10.1007/s10676-020-09568-6).

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., and Collignon, S. E. 2017. "Exposing Others' Information on Online Social Networks (OSNs): Perceived Shared Risk, Its Determinants, and Its Influence on OSN Privacy Control Use," *Information and Management* (54:7), Elsevier B.V., pp. 851–865. (https://doi.org/10.1016/j.im.2017.01.001).

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., and Janowski, T. 2020. "Data Governance: Organizing Data for Trustworthy Artificial Intelligence," *Government Information Quarterly* (37:3), Elsevier, p. 101493. (https://doi.org/10.1016/j.giq.2020.101493).

Laatikainen, G., Kolehmainen, T., and Abrahamsson, P. 2021. "Self-Sovereign Identity Ecosystems: Benefits and Challenges," in *12th Scandinavian Conference on Information Systems*, Orkanger, Norway, pp. 1–16.

Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., Kettunen, A., and Abrahamsson, P. 2021. "Towards a Trustful Digital World: Exploring Self-Sovereign Identity Ecosystems," in *PACIS 2021 Proceedings*, Dubai, UAE, pp. 1–16. (https://arxiv.org/abs/2105.15131%0Ahttp://arxiv.org/abs/2105.15131).

Lesnykh, A. 2011. "Data Loss Prevention: A Matter of Discipline," *Network Security* (2011:3), pp. 18–19. (https://doi.org/10.1016/S1353-4858(11)70028-9).

Lin, J., and Halloran, S. 2021. "Study: Effectiveness of Apple's App Tracking Transparency," *Lockdown Privacy*, , September 22. (https://blog.lockdownprivacy.com/2021/09/22/study-effectiveness-of-apples-app-tracking-transparency.html).

Makridis, C. A. 2021. "Do Data Breaches Damage Reputation? Evidence from 45 Companies between 2002 and 2018," *Journal of Cybersecurity* (7:1), pp. 1–8. (https://doi.org/10.1093/cybsec/tyab021).

Mühle, A., Grüner, A., Gayvoronskaya, T., and Meinel, C. 2018. "A Survey on Essential Components of a Self-Sovereign Identity," *Computer Science Review* (30), pp. 80–86. (https://doi.org/10.1016/j.cosrev.2018.10.002).

Politou, E., Alepis, E., and Patsakis, C. 2018. "Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions," *Journal of Cybersecurity* (4:1), pp. 1–20. (https://doi.org/10.1093/cybsec/tyy001).

Power, D. J. 2016. "'Big Brother' Can Watch Us," *Journal of Decision Systems* (25), Taylor & Francis, pp. 578–588. (https://doi.org/10.1080/12460125.2016.1187420).

Richardson, V. J., Smith, R. E., and Watson, M. W. 2019. "Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches," *Journal of Information Systems* (33:3), pp. 227–265. (https://doi.org/10.2308/isys-52379).

Royakkers, L., Timmer, J., Kool, L., and van Est, R. 2018. "Societal and Ethical Issues of Digitization," *Ethics and Information Technology* (20:2), Springer Netherlands, pp. 127–142. (https://doi.org/10.1007/s10676-018-9452-x).

Samtani, S., Chinn, R., Chen, H., and Nunamaker, J. F. 2017. "Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence," *Journal of Management Information Systems* (34:4), Routledge, pp. 1023–1053. (https://doi.org/10.1080/07421222.2017.1394049).

Smith, T. J. 2020. "Haystack in a Hurricane: Mandated Disclosure and the Sectoral Approach to the Right to Privacy," *Yale Journal on Regulation* (37), p. 25.

Solove, D. J. 2007. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* (44:May), pp. 1–23. (https://doi.org/10.2139/ssrn.998565).

Steffel, J. 2019. "The Time Between the Theft and the Injury: Standing Requirements Based on a Future Risk of Identity Theft After a Data Breach," *University of Cincinnati Law Review* (88:4), p. 1189.

Stepney, C. 2019. "Actual Harm Means It Is Too Late: How Rosenbach v. Six Flags Demonstrates Effective Biometric Information Privacy Law," *Loyola of Los Angeles Entertainment Law Review* (40:1), pp. 51–87.

Sunda, K. 2020. "Online Privacy - Self-Sovereign Identity," *Journal of Information System Security* (16:2), pp. 121–135.

Sunyaev, A. 2020. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, Cham: Springer International Publishing. (https://doi.org/10.1007/978-3-030-34957-8).

Thompson, R. M. 2014. "The Fourth Amendment Third-Party Doctrine," Washington, D.C.

W3C. 2019. "Terminology," *Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web*, , November 19. (https://www.w3.org/TR/vc-data-model/#terminology).

Yang, X., and Li, W. 2020. "A Zero-Knowledge-Proof-Based Digital Identity Management Scheme in Blockchain," *Computers & Security* (99), p. 102050. (https://doi.org/10.1016/j.cose.2020.102050).

Young, J. A., Biros, D. P., Schuetzler, R. M., Smith, T. J., Stephens, P. R., Syler, R. A., and Zheng, S. H. 2020. "When Programs Collide: A Panel Report on the Competing Interests of Analytics and Security," *Communications of the Association for Information Systems* (46:5), pp. 584–602. (https://doi.org/10.17705/1cais.04624).

Young, J. A., and Farshadkhah, S. 2021. "Improving Anonymous Whistleblower Credibility with Self-Sovereign Identity," in *Proceedings of the 2021 IFIP 8.11/11.13 Dewald Roode Information Security Research Workshop*, San Antonio, Texas.

Young, J. A., Smith, T. J., and Zheng, S. H. 2020. "Call Me BIG PAPA: An Extension of Mason's Information Ethics Framework to Big Data," *Journal of the Midwest Association for Information Systems* (2020:2), pp. 17–41. (https://doi.org/10.17705/3jmwa.000059).

Zuboff, S. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* (30:1), pp. 75–89. (https://doi.org/10.1057/jit.2015.5).