Self-Sovereign Identity or SSI technology in identity management for financial cooperatives

Wilman Enrique Navarro Mejía [1], Yennifer Bejarano [2] , Astrid Ramírez Valencia [3]

[1] Universidad Francisco José de Caldas, Bogotá, Colombia,
ID:https ://orcid.org/0000-0002-8796-776

[2] Universidad Francisco José de Caldas, Bogotá, Colombia,
ID : https://orcid.org/0009-0007-0913-8830

[3] Universidad Francisco José de Caldas, Bogotá, Colombia,
https://orcid.org/0000-0002-3025-59i2,
ID: https://orcid.org/0009-0007-0913-8830

Summary

Self - Sovereign Identity Identity (hereinafter SSI) represents a disruptive innovation in digital identity management, enabling individuals and organizations to have direct and secure control over their own personal data. This technology offers substantial benefits in terms of privacy, information security, and trust in digital environments. The determining factors for its adoption relate to organizational, social, and environmental aspects, as well as the suitability of technological ecosystems for its implementation. The analysis reveals concrete benefits associated with the adoption of SSI, such as increased operational efficiency, enhanced privacy, improved digital trust, and expanded collaboration among organizations.

The scientometric and bibliometric process was carried out by reviewing digital repositories such as Scopus , Web of Science , Dimensions , Lens and OpenAlex , from which we kept the results obtained in Scopus , through two separate searches, the first by means of the equation " Self Sovereign Identity " with the variables " article title , abstract keywords ", yielding a data of 1192 documents; on the other hand, the second search was with " Self Sovereign Identity OR financial cooperatives ", providing a data set of 9360 documents. The
The processing of the retrieved data was carried out using "VOSviewer", leaving a final data that is reflected in the bibliographic references of this article.

From a theoretical perspective, this study contributes to the advancement of technology adoption frameworks by integrating ecosystem elements and individual characteristics. In practical terms, it offers key recommendations for organizational leaders and policymakers interested in promoting the effective implementation of SSI solutions.

Keywords: Self-sufficient identity (SSI), Decentralized identity, Biometrics, Financial technology

1. Introduction

The management of existing identity infrastructures often fails to meet evolving demands for privacy, security, and trust [1]. This challenge underscores the urgent need for new digital identity systems that adapt to dynamic social and technological contexts.

Adopting digital technologies generates social benefits, such as increased connectivity, financial inclusion, and access to essential everyday services. However, the growing reliance on digital ecosystems has exposed individuals and organizations to serious risks, including identity theft, financial fraud, data breaches, and abusive surveillance practices [2]. Therefore, a new approach to digital identity management is paramount in contemporary life.

The adoption of SSI technology, for financial organizations with a cooperative focus, is a timely alternative due to their organizational structures, regulatory frameworks and the services they offer.

Therefore, the purpose of this study was to investigate the background and potential outcomes of SSI technology adoption, focusing on adoption factors identified in the research, such as organizational, social, and environmental aspects, as well as suitability within technological ecosystems.

Our contribution begins by promoting the literature on SSI technology adoption for governance integration in financial cooperative organizations. We then present traditional models for identity technology adoption and finally provide an alternative model for SSI technology adoption. This provides relevant information for managers and policymakers to support strategic decision-making and mitigate adoption-related risks. The proposal serves as a guide for the organizations under study, namely, financial cooperatives.

The article was structured based on a qualitative approach, from a digital documentary review retrieved from widely recognized repositories such as Scopus and WoS, of a corporate nature, on the other hand, they were complemented with Dimensions, OpenAlex, and Lens; as open source or open science consultation repositories.

2. Existing technologies for identification and authentication

2.1. Autonomous Identity or SSI

Based on the information gathered in this study, we can state that it can be considered a framework for legitimizing human-centered technologies and standards, for personal or organizational application; users own and control their own identity and the personal data associated with it [3]. SSI enables human-centered identity management by providing users with a decentralized digital identity [4]. Equally important, it can be viewed as a digital identity infrastructure, a product that provides secure, reliable, and private data storage and communication [5].

Key components of SSI include a digital wallet [6], verifiable credentials [7], decentralized identifiers, and a verifiable data ledger. Finally, it should be noted that many SSI adoptions are based on distributed ledger technologies, often referred to as blockchain technology.

Adopting SSI technology requires a technological system with distinct actors and specific roles that form the operational technology triad, enabling the holder, issuer, and verifier to function efficiently [8]. Holders must request credentials as a digital representation, and issuers store them in their technological systems. When requested by the verifier, holders can approve the request and present the credentials for verification and confirmation. Issuers define the credentials, their meaning, and the verification method. Verifiers request the credentials they need and then follow their own policy to verify their authenticity [2].

In SSI technology, trust between actors is referenced with peer-to-peer transactions, certified by the technology that provides data storage, exchange and communication [9], and on the other hand, governance guidelines; which consist of commercial, legal and technical rules and policies to manage, in particular commercial, legal and technical policies to issue, maintain and verify credentials [10] .

Understanding SSI requires a consistent approach to technological infrastructure and governance structures. This sociotechnical approach recognizes that SSI operates at the intersection of technology and institutional governance, shaping trust, interoperability, and adoption dynamics [11].

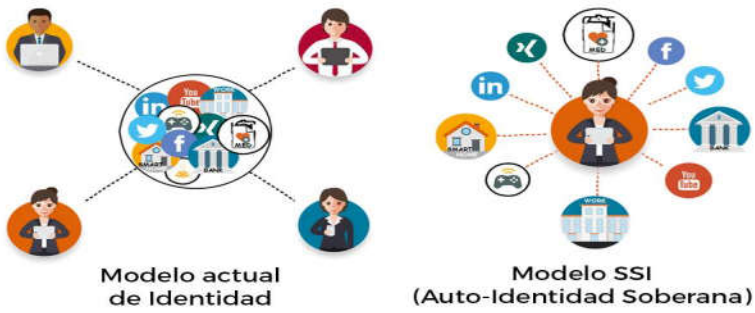

Image 1. Current identity versus SSI[1]

[1]https://resilientedigital.com/que-es-la-auto-identidad-soberana-ssi-self-sovereign-identity/

2.2. Theories of technology adoption

The adoption of SSI should be supported by the various existing approaches to identity technologies, which we summarize as technical support for its understanding.

Initially, we addressed the Technology/Organization/Environment (TOE) framework [12],1990, and the Diffusion of Innovations (DOI) theory (Rogers, 2003), both of which are widely used, even as complements to one another. Specifically, the TOE framework posits that technology adoption is affected by technological, organizational, and environmental factors, while the five characteristics of innovation suggested by DOI (relative advantage, complexity, compatibility, testability, and observability) are considered part of the technological factors. It is important to note that these two theories do not consider the human characteristics and behaviors that play a fundamental role in technology adoption.

Successful adoption of Self-Sovereign Identity (SSI) must be based on studies of individual technology acceptance, adoption behavior, behavioral intention, and attitudes toward technology. These aspects are typically analyzed through established theoretical frameworks, such as:

- The Theory of Reasoned Action [13].
- The Theory of Planned Behavior [13].
- The Technology Acceptance Model (TAM) [14].
- The Unified Theories of Technology Acceptance and Use I and II (UTAUT and UTAUT2) [15].

These models explain that the determining factors of technological acceptance include:

- Perceived utility.
- The perceived ease of use.
- The intended use [14].
- Performance expectancy, effort expectancy, social influence, and enabling conditions [15].

2.3. Analytical framework for the adoption of SSI

Given the inherent complexity of Self-Sovereign Identity (SSI), its technological adoption requires an adaptive and contextual approach [16]. Inspired by established technology acceptance theories and factorial models [17], we propose an analytical framework that considers four interrelated categories of factors that influence SSI adoption:

a) Individual factors

Individuals are the final agents in adoption decisions. Aspects such as risk-taking, openness to innovation, and technological experience affect how decision-makers evaluate and implement SSI solutions [18].

b) Organizational factors

Determinants of internal readiness and strategic priorities. Based on the TOE framework and DOI theory, factors such as organizational culture, leadership attitude towards innovation, and the availability of technical and financial resources influence [12].

c) Ecosystem factors

These include available technological infrastructures, governance models for SSI, and the level of interoperability. These elements define the technical and political feasibility for adoption.

d) Environmental and social factors

Such as regulatory frameworks, institutional pressure, and public sector commitment, which condition the pace and form of adoption [19].

The adoption of Self-Sovereign Identity (SSI) is profoundly influenced by exosystemic and environmental factors that determine both its viability and large-scale implementation. From an ecosystem perspective, this technology depends on coordination among various actors—issuers, verifiers, and holders—who, together, enable reliable and secure identity transactions. Elements such as technological complexity, as highlighted by Diffusion of Innovation (DOI) theory, affect organizations' perceptions of feasibility, while governance structures, responsible for defining rules and responsibilities, remain an underdeveloped aspect in the specialized literature [20]. Regarding the external environment, environmental factors play a key role in establishing the framework within which organizations operate; While competitive pressure from the sector can accelerate the adoption of SSI as a differentiation strategy, regulatory frameworks ensure compliance in terms of privacy and data protection, and market conditions, customer expectations, emerging innovations and the economic situation all directly affect the motivation and speed with which organizations decide to adopt this technology [12].
Self-Sovereign Identity (SSI) provides companies with the opportunity to innovate by developing services that prioritize privacy, strengthen data security, and give users greater control over their personal information [21]. Furthermore, the implementation of SSI allows for optimized operational efficiency and minimized risks inherent in data management, thanks to the use of decentralized identity protocols that eliminate dependence on intermediaries and reduce vulnerabilities.

At the ecosystem level, the adoption of SSI progressively drives digital infrastructure. By integrating into an SSI network, organizations, service providers, and users contribute to expanding the participant base, which improves interoperability and fosters smoother identity verification across diverse platforms [22]. This collaborative growth not only increases the value of the system for all stakeholders but also strengthens trust and efficiency in the secure exchange of data within the digital ecosystem.

The social and environmental factors allow the implementation of Self-Sovereign Identity (SSI) to contribute to the sustainable modernization of identity management by replacing paper-based processes with digital solutions, thus decreasing the need for documents and reducing the environmental impact of traditional physical methods. This technology also empowers users by giving them greater control over their personal information, thereby promoting privacy protection, data security, and individual ownership. By combining digital efficiency with environmental responsibility, SSI is positioned as a key tool for advancing towards more sustainable and inclusive identity management [23].

Integrating factors and impacts at multiple levels provides a response to current identity gaps and presents a comprehensive view on the adoption of Self-Sovereign Identity (SSI). This approach underscores the interdependence between technological, organizational, and social dimensions, offering valuable insights into how SSI can contribute to creating a safer, more efficient, and more sustainable digital environment.

3. Guidelines for the adoption of SSI

Due to the emergent nature of the SSI phenomenon, a pre-adoption analysis of the implementation context is essential. This approach allows for the flexibility and openness necessary to investigate SSI using empirically rich and detailed qualitative data [24]. Reliable data collection tools, such as interviews, fieldwork, or expert consultation, are also necessary. This provides a broad understanding of the topic while generating valuable data [25]. Furthermore, semi-structured interviews with experienced SSI professionals are crucial for a deeper understanding of the specific aspects of its adoption.

3.1. Data collection

For data collection, information is drawn from the compiled and reviewed literature on SSI technologies. It is recommended to conduct targeted sampling involving individuals and organizations related to SSI in order to articulate diverse perspectives. This also allows for collaboration in the development of standardization for SSI adoption, as well as with Standards Development Organization (SDO) initiatives, participation in discussions with industry experts, and facilitation of collaboration among peers and SSI infrastructure providers. These interactions allow for the exploration of the background and outcomes of SSI adoption in real-world contexts.

Furthermore, fieldwork allows for the collection of data such as dates, sources, participants, and previously unconsidered perspectives, as well as messages, audiovisual material, web activities, and more. This interaction provides information on the contribution to a governance framework for a UNICEF-driven SSI ecosystem, offering key insights into governance challenges [26].

Finally, another important aspect to consider concerns digital wallets. Their trust and acceptance must be linked to ecosystem governance and user adoption. This requires ongoing training on SSI technology, complemented by proficiency in managing the "TrustOverIP" technology model.

3.2. Data Analysis

Managing the variety of collected data is a complex activity, requiring its presentation in diverse formats, including video, images, or text. Therefore, data analysis must be performed using both qualitative and quantitative processing applications, including open, axial, and theoretical coding analyses; in conclusion, it should be a data analytics approach using generative artificial intelligence algorithms.

Open coding emphasizes key aspects for SSI adoption by labeling text segments with updatable and regenerative codes. Applying the constant comparative method, which allows extracting only what is needed from the text, ensures that the codes capture accurate meanings.

Axial coding establishes patterns, relationships, and causal links between codes, allowing for the creation of related open codes to categorize different aspects of the SSI adoption phenomenon. In short, it is a hierarchical coding process for a better understanding of interrelated variables. Finally, theoretical coding establishes the conceptual framework that provides a comprehensive understanding of SSI adoption.

3.3. Technology in Financial Cooperatives

Cooperative organizations are situated within the framework of the solidarity economy, which has seen significant development in Latin America. This economy offers an alternative approach to classical economics and has several interpretations. In Argentina, it is known as the labor economy; in Ecuador, it is called the popular economy; in Brazil, it is the Solidarity Economy and Third Sector; in Peru, it is the informal economy; and in Colombia, it is simply the Solidarity Economy. This demonstrates the multifaceted nature of the concept. Within the organizational universe of cooperatives, there are different approaches depending on their founding mission, and it is within this context that our study is framed, specifically within the "financial cooperativism" sector. We can therefore assume that, as cooperative organizations, they exhibit particular characteristics in various aspects, such as service provision, organizational structure, resource management, and the adoption of ICT and digital technologies.

Financial cooperatives in Colombia play an important role in the country's economic and social development, offering a distinct alternative to traditional financial institutions. They work to meet the needs of their members by providing a wide range of financial services, including savings, loans, insurance, and other forms of financing.

With technological advancements and the sensitivity of the information handled by these organizations, it is essential to control access for all employees in their operational management, with a proper segregation of duties that allows for assigning the permissions and access that users actually need. This article delves into alternative "Identity" technologies for Financial Cooperatives to manage identities, vulnerabilities, and threats that affect information security professionals, managers, and clients of these organizations.

Financial cooperatives face significant risks due to the volume of daily financial transactions and the sensitivity of the information they handle, making them attractive targets for cybercriminals. Therefore, it is essential that financial cooperatives implement robust access control strategies. This process helps protect the organization's assets, and effective identity management ensures that only authorized individuals have access to systems and resources. These strategies should also encompass employee education and awareness, as well as the adoption of advanced threat detection and prevention technologies. Furthermore, continuous and rigorous monitoring of information systems is crucial, with regular audits to identify potential vulnerabilities and ensure a secure environment.

Colombia has 4,000 cooperatives overseen by the Superintendency of the Solidarity Economy, but a total of 10,500 are registered with the country's Chambers of Commerce. The Colombian Confederation of Cooperatives (Confecoop) indicates that there are 3,200 cooperatives with 6.3 million members, benefiting more than 20 million people. These cooperatives operate in diverse economic sectors, including finance, with 185 entities and assets of 14 trillion pesos, or 3.5 billion dollars, representing a significant sector of the Colombian economy. Therefore, our subject of study is highly relevant. However, it lags behind in the management of information and communication technologies, as indicated by the 2023 report "Digital Transformation in the Solidarity Sector", which points out that only 25% of small cooperatives have started digitization processes, mainly due to a lack of resources and technical knowledge, especially in relation to digital identity services, compared to their competitors, such as traditional banking.

4. Analysis of general aspects

Our study determined that achieving positive results from implementing ISS technology is a multifaceted process characterized by continuous interaction

between organizations and the broader ecosystem. Based on our analysis, we identified key antecedents and potential outcomes of adopting an SSI.

The adoption of SSI is influenced by multiple interrelated factors that determine the readiness and capacity of organizations, ecosystems, and individuals to adopt the technology. We were able to identify the antecedents that shape the adoption process, such as organizational antecedents, social antecedents, ecosystem-specific antecedents, and individual-level antecedents, which we briefly describe below:

- Our analysis revealed that several organizational factors influence the adoption of SSI. First, senior management attitude proved to be a decisive factor, as an organization's financial situation plays a crucial role. It is important to note that organizations with financial constraints may delay SSI adoption due to insufficient budgets. Organizational culture, innovation, and size also influence SSI adoption. Organizations with a culture of innovation are more likely to adopt new technologies, and larger organizations with dedicated R&D budgets can absorb greater risks.

- The age and size of an organization further influence the adoption of SSI, as older organizations face the challenges of consolidating pre-existing systems, while younger and smaller organizations typically have fewer legacy systems, simplifying SSI adoption. Similarly, technological competence also plays a key role in SSI adoption, as organizations with advanced technical skills can create customized solutions when predefined tools are unavailable, allowing for the integration of an SSI into legacy systems and contributing to technological development.

- A Secure Security Initiative (SSI) can improve privacy and security, privacy awareness, and regulatory compliance. Country- and culture-specific characteristics include regulations and laws, such as Data Protection Standards, Data Governance, and national laws, with requirements for data management and sharing. To mitigate these challenges, SSI allows customers to securely control their data while reducing the burden of data storage and management for organizations; however, the entire process must be aligned with the corporate governance framework.

- Organizations with skilled digital professionals are more likely to adopt a Security Information System (SIS), while those with limited digital literacy face greater barriers due to their lack of knowledge of digital tools and concerns about privacy and security; in other words, the level of digital knowledge and the need for verifiable data determine the adoption of an SIS.

- Emerging technology plays a fundamental role; for contexts with digital identification services, SSI-based identification services are expanding. The adoption of SSI requires the coordination of multiple actors and components, including diverse user interfaces for issuers, verifiers, and holders, as well as

data registries, backup mechanisms, and data schemas—in other words, it enables full technological convergence.

- The development of digital wallets and other user interfaces requires synchronous communication with the target user group during development, as interoperability between diverse SSI solutions is essential due to the cross-sector and cross-border applications of the technology. Issued digital identities must function seamlessly in sectors such as healthcare, education, justice, and, in general, across all productive sectors that handle sensitive data.

- Legal and technical business policies are fundamental to adoption decisions, and organizations must consider regulations, compliance requirements, and contractual conditions to uphold governance principles such as transparency, portability, and consent when offering privacy-protecting services, in order to join ecosystems with similar guiding principles. Ultimately, the credibility of actors involved in ecosystems of prestigious institutions and large corporations inspires greater trust and fosters increased participation. Conversely, ecosystems led by less established actors may face challenges due to perceived risks related to sustainability and reliability.

Aspect	Feature description
General Analysis	The adoption of SSI is a multifaceted process influenced by organizational, social, ecosystem, and individual factors; it requires the support of senior management and financial resources. A culture of innovation and the size of the organization also play a significant role.
Organizational Factors	Organizations with a culture of innovation and advanced technical skills are more likely to adopt Secure Software Integration (SSI), and technology allows for the integration of SSI into outdated organizational systems. Adopting SSI improves privacy and security, reduces risks such as fraud, and fosters innovation. Organizational digital wallets based on SSI enhance employee privacy and security.
Social and Ecosystem Factors	Digital literacy and the need for verifiable data are key drivers for the adoption of Secure Situations (SSI). Interoperability between SSI solutions is essential for cross-sector and cross-border applications. SSI improves living conditions through secure and private digital interactions. Credit profiles become portable, facilitating access to financial services. Adopting SSI facilitates new strategic alliances and improves collaborative performance, enabling organizations to open new markets and transform ecosystem structures.

Table No. 1. Description of the aspects of the SSI

4.1. Possibilities of organizational outcomes

The adoption of Secure Securities (SSI) has several potential organizational benefits. The primary focus of SSI is to improve the privacy and security of services

offered by organizations, while simultaneously reducing risks such as fraud and misuse of the service. This is especially relevant in the financial sector, where, for example, financial cooperatives seek to mitigate cybercrime and identity fraud. Organizational digital wallets based on SSI enhance the privacy and security of employees acting on behalf of their employers.

Furthermore, it is important to note that the SSI has adopted the “LEI” prototype, developed by the Global Legal Entity Identifier Foundation, whose objective is to establish a chain of trust for organizational identity.

Adopting emerging technologies fosters innovation, leading to the development of new products and services, which can improve financial performance and competitive advantage. One example is lifetime SSI-based reputation systems, which allow organizations to issue digital credentials recognizing the achievements of customers and employees. These credentials can increase employees' value in the job market and provide professional motivation.

SSI can simplify compliance processes. For example, when an organization implements KYC (Know Your Customer) verification through SSI, it can choose to transfer responsibility for managing sensitive customer data from the organization to the customers themselves. This reduces compliance burdens related to data security and privacy regulations. Furthermore, automating processes through digital documents can generate operational efficiencies and cost savings by replacing manual tasks.

4.2. Possibilities for social analysis

The adoption of Secure Information Systems (SIS) also contributes to social value, particularly through its ability to improve living conditions via secure and private digital interactions. By allowing data owners to maintain control over their data, SIS enhances digital interactions. SIS drives digital transformation in various sectors, such as education, healthcare, government, and tourism, through document digitization and the automation of processes like identification and authorization.

People's credit profiles are becoming portable, rather than confined to a centralized office, giving citizens broader access to financial services through a digital identity issued by the government. For example, digital wallets could make customer profile management systems obsolete by enabling real-time data verification from users' wallets, thus reducing the need for customer service staff.

4.3. Possibilities for ecosystem analysis

Organizations' decisions to adopt SSI and join an ecosystem significantly impact its overall structure and dynamics, as organizations that join an SSI ecosystem facilitate the formation of new strategic alliances, foster joint learning, and improve collaborative performance.

Organizations that join an SSI ecosystem can open new markets and transform existing structures. For example, if an organization in an SSI-based organizational identity ecosystem issues SSI-enabled work certificates to its employees, it could create new reputation-based service markets.

5. Conclusions

- Implementing an SSI involves carrying out a comprehensive process with four dimensions: human and technological resources, institutional commitment, and short, medium, and long-term vision.
- Individual, organizational, environmental and social factors, ecosystem factors, and SSI factors must be included in the implementation.
- Adopting SSI offers economic benefits, strategic alliances, and the creation of new market structures.
- These strategic alliances promote shared learning and improved collective performance.
- The inclusion of SSI allows for greater long-term viability of the organization.

References

[1] S. Masiero, V. Arvidsson. (2021). “Degenerative outcomes of digital identity platforms for development” Information Systems Journal, 31 (6) (2021), pp. 903-928, 10.1111/isj.12351 .

[2] V. Schlatt, J. Sedlmeir, S. Feulner, N. Urbach. (2022). “Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity” Information & Management, 59 (7) (2022), Article 103553, 10.1016/j.im.2021.103553 .

[3] N. Naik, P. Jenkins. (2020) “Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology” 2020 8th IEEE international Conference on mobile cloud computing, services, and Engineering (MobileCloud), 10.1109/MobileCloud48802.2020.00021 .

[4] M. Ferdous, U. Cali, U. Halden, W. Prinz. (2023). Leveraging self-sovereign identity & distributed ledger technology in renewable energy certified ecosystems. J. Clean. Product., 422, Article 138355. https://doi.org/10.1016/j. jclepro.2023.138355.

[5] A. Zwitter, O. Gstrein, E. Yap. (2020). “Digital identity and the blockchain: Universal identity management and the concept of the “self-sovereign” individual.” Frontiers in Blockchain, p. 26, 10.3389/fbloc.2020.00026 .

[6] M. Kuperberg. (2020) “Blockchain-based identity management: A survey from the enterprise and ecosystem perspective” IEEE Transactions on Engineering Management, 67 (4), pp. 1008-1027, 10.1109/TEM.2019.2926471

[7] W3C DID, DIDs. https://www.w3.org/TR/did-core/ (2022). Google Scholar

[8] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell, D. Reed. (2019). The trust over IP stack. IEEE Communications Standards Magazine, 3(4), 46–51. https:// doi.org/10.1109/MCOMSTD.001.1900029

[9] M. Lacity, M. Carmel. “Self-Sovereign Identity and Verifiable Credentials in Your Digital Wallet” MIS Quarterly Executive, https://aisel.aisnet.org/misqe/vol21/iss3/6

[10] R. Joosten, S. Den Breeijen, D. Reed. “Decentralized SSI Governance, the missing link in automating business decisions.” https://doi.org/10.13140/RG.2.2.35491.68640

[11] G. Laatikainen, T. Kolehmainen, P. Abrahamsson. (2021) “Self-sovereign identity ecosystems: Benefits and challenges” Scandinavian conference on information systems, Vol. 10. https://aisel.aisnet.org/scis2021/10

[12] Tornatzky, L. Fleischer, M. “The processes of technological innovation” Lexington Books, Lexington, MA (1990).

[13] I. Ajzen. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.

[14] F. Davis. (1989). A technology acceptance model for empirically testing new end-user information systems: Theory and results. Massachusetts Institute of Technology (1986). MIS Quarterly https://dspace.mit.edu/bitstream/handle/1721.1/15192/1492713 7-MIT.pdf, 2023.

[15] V. Venkatesch. “User Acceptance of Information Technology: Toward a Unified View”, https://www.researchgate.net/publication/220259897_User_Acceptance_of_Information_Technology_Toward_a_Unified_View.

[16] O. Gstrein, D. Kochenov. (2020). Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world? Frontiers in Blockchain, 3, 10. https://doi.org/10.3389/fbloc.2020.00010 .

[17] O. Pitkänen. (2003) “Assessing legal challenges on the mobile Internet” Int. J. Electron. Commer., 8 (1), pp. 101-120, 10.1080/10864415.2003.11044284

[18] A. Benlian, T. Hess. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52(1), 232–246. https://doi. org/10.1016/j.dss.2011.07.007.

[19] Hickman, N. (2022). Overcoming human harm challenges in digital identity ecosystems. https://trustoverip.org/wp-content/uploads/Overcoming-Human-Harm-Ch allenges-in-Digital-Identity-Ecosystems-V1.0-2022-11-16.pdf. IATA Travel Passport. (2021).

[20] G. Laatikainen, T. Kolehmainen, P. Abrahamsson. (2021). “Self-sovereign identity ecosystems: Benefits and challenges” Scandinavian conference on information systems, Vol. 10. https://aisel.aisnet.org/scis2021/10

[21] R. Soltani, U. Nguyen, A. An. (2021). “A survey of self-sovereign identity ecosystem” Secur. Commun. Network., 2021, Article e8873429, 10.1155/2021/8873429

[22] O. Henfridsson, B. Bygstad. (2013). The Generative Mechanisms of Digital Infrastructure Evolution. MIS Quarterly, 37(3), 907–931. https://www.jstor.org/stable/43826006.

[23] J. Glockler, J. Sedlmeir, M. Frank, G. Fridgen. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Information Bus Sys. Eng., 66(4), 421-440. https://doi.org/ 10.1007/s12599-023-00830-x

[24] A. Edmondson, S. McManus. (2007). Methodological fit in management field research. Academic Manag. Rev., 32(4). https://doi.org/10.2307/20159361. Article 4. JSTOR.

[25] M. Myers, M. Newman. (2007). “The qualitative interview in IS research: Examining the craft” Informatica. Organizational., 17 (1) pp. 2-26.

[26] M. Sroor, N. Hickman, G. Kolehmainen, G. Laatikainen, P. Abrahamsson. (2022). “How modeling helps in developing self-sovereign identity governance framework: An experience report” Procedia Computer Science, 204, pp. 267-277

[27] A. Aswan. (2019). “Transaksi perbankan melalui internet banking,” Solusi, vol. 17, no. 3, pp. 317–335. 10.36546/solusi.v17i3.220.

[28] R. Lai, T. Wangy, Y. Chen, (2023) “Using grid symmetric encryption for location privacy protection”, J. Commun., vol.13, no.11, pp. Apocalypse 673-678.

[29] R. Adner. (2017). Ecosystem as Structure: An Actionable Construct for Strategy. Journal of Management, 43(1), 39-58. https://doi.org/10.1177/0149206316678451 .

[30] I. Ajzen, M. Fishbein. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

[31] A. Aswan. (2019). “Transaksi perbankan melalui internet banking,” Solusi, vol. 17, no. 3, pp. 317–335, 10.36546/solusi. v17i3.220.

[32] P. Beynon-Davies. (2018). Characterizing business models for digital business through patterns. Int. J. Electron. Commer., 22(1). https://doi.org/10.1080/ 10864415.2018.1396123. Article 1.

[33] D. Birch. (2018). Digital identity and davos. Retrieved 2024 https://www.linkedin.com/ pulse/digital-identity-davos-david-birch/.

[34] A. Caputo, S. Pizzi, M. Pellegrini, M. Dabic. (2021). Digitalization and business models: Where are we going? A science map of the field. J. Bus. Res., 123, 489-501. https://doi.org/10.1016/j.jbusres.2020.09.053

[35] Y. Chen, L, Chen, S. Zou, H. & Hou. (2021). Easy to start, hard to persist: Antecedents and outcomes of entrepreneurial persistence in online marketplaces. Int. J. Electron. Commer., 25(4), 469-496. https://doi.org/10.1080/10864415.2021.1967003

[36] P. Darke, G. Shanks, M. Broadbent. (1998). Successfully completing case study research: Combining rigor, relevance and pragmatism. Information Systems Journal, 8(4), 273-289. https://doi.org/10.1046/j.1365-2575.1998.00040.x .

[37] Deloitte. (2020). FEBRABAN Banking Technology Survey. Accessed: April. 17, 2024.
https://www2.deloitte.com/content/dam/Deloitte/br/Documents/_nancialservices/2020%20FEBRABAN%20Banking%20Technology%20Survey.pd

[38] Digital Europe. (2023). The ecosystem digital product passport (CIRPASS) prepares the ground for gradual piloting and deployment of the digital product passports (DPPs). https://www.digitaleurope.org/projects/digital-product-passport/.

[39] Eisenhardt. (1989). Building theories from case study research. Academic Manag. Rev., 14(4), 532-550. https://www.jstor.org/stable/258557 .

[40] European Commission. (2021). https://commission.europa.eu/strategy-and-policy/pri orities-2019-2024/europe-fit-digital-age/european-digital-identity_en.

[41] European Commission. (2023). EU Digital Identity Wallet Pilot implementation. https://digi tal-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation.

[42] Finnish Tax Administration. (2022). Digitalized accounting systems ease the administrative burden of business taxpayers. https://www.vero.fi/en/About-us/finnish-tax-administration/operations/real-time-economy/.

[43] A. Giannopoulou, F. Wang. (2021). Self-sovereign identity. Internet Policy Review, 10 (2). https://policyreview.info/glossary/self-sovereign-identity. Article 2.

[44] M. Glaude. (2023). SSI Orbit podcast [Broadcast] https://northernblock.io/podcasts/. Global Legal Entity Identifier Foundation. https://www.gleif.org/en .

[45] Good Heath Pass. (2021). The good health pass collaborative. https://www.goodhealthpass.org/.

[46] T. Guggenberger, D. Kühne, V. Schlatt, N. Urbach. (2023). Designing a crossorganizational identity management system: Utilizing SSI for the certification of retailer attributes. Electron. Market., 33(1), 3. https://doi.org/10.1007/s12525-02 3-00620-z.

[47] O. Gstrein, D. Kochenov. (2020). Digital identity and distributed ledger technology: Paving the way to a neo-feudal brave new world? Frontiers in Blockchain, 3, 10. https://doi.org/10.3389/fbloc.2020.00010 .

[48] IATA travel pass. https://www.flypgs.com/en/iata-tr avel-pass.

[49] M. Jacobides, C. Cennamo, A. Gawer. (2018). Towards a theory of ecosystems. Strateg. Manag. J., 39(8). https://doi.org/10.1002/smj.2904. Article 8.

[50] M. Kwang. (2016) Agent-based cloud computing. IEEE Trans. Serv. Computing 5 (4) (2011) 564-577.

[51] Real Time Economy. (2023) “eReceipts and digital wallets support automated cost management approaches” https://www.yrityksendigitalous.fi/en/blogs/ereceipts-support-automated-cost-management-approaches

[52] Roger, (2003). https://www.taylorfrancis.com/chapters/edit/10.4324/9780203887011-36/diffusion-innovations-everett-rogers-arvind-singhal-margaret-quinlan

[53] A. Satybaldy, M. Ferdous, M. Nowostawski. (2024) “A taxonomy of challenges for self-sovereign identity systems” IEEE Access.

[54] Swiss Finance Council. (2020). “Getting Ready for the '20s-Technology and the Future of Global Banking.” April. 15, 2024. https://www.swiss_nancecouncil.org/images/SFC_Discussion_Paper_2020.pd

[55] W. Abramson. N. Hickman (2021). Evaluating trust assurance in Indybased identity networks using public ledger data. Front. Blockchain, 4, 18. https:// doi.org/10.3389/fbloc.2021.622090

[56] P. Wang, De Filippi “Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion” Front. Blockchain, 2 (2020), 10.3389/fbloc.2019.00028

[57] P. Windley. “Digital identity” O'Reilly Media, Inc (2005).