Administrative Law and Procedure

UDC 004.9:342.7

DOI https://doi.org/10.5281/zenodo.17532852

Self-sovereign identity as the basis for digital asset management in the Web3 environment

Oleksandr Tuholukov,

Chief Business Officer, NOTA Digital Currencies Research Center Inc.,

5307 Marconi Ave, Apt 22, Carmichael, CA 95608, USA,

https://orcid.org/0009-0008-3661-764X

Dmytro Lyushenko,

CEO, NOTA LLC, 5307 Marconi Ave, Apt 22, Carmichael, CA 95608, USA,

https://orcid.org/0009-0003-9180-0934

Accepted: 17.10.2025 | Published: 30.10.2025

Abstract. The rapid development of decentralized technologies and blockchain is transforming the methods of authentication, data management and the implementation of digital human rights, which actualizes the need to form a new identity paradigm based on user autonomy and trustful interaction without intermediaries. The purpose of this article is to substantiate self-sovereign identity as the foundation of trust and digital asset management within the Web3 ecosystem. The research methodology combines comparative legal and formal-dogmatic analysis, structural-functional modeling of the three-way interaction among issuer, holder, and verifier, as well as a problem-oriented review of the technical standards and practices of early platforms (Sovrin, uPort). It is demonstrated that the emergence of self-sovereign identity is a natural response to the shortcomings of

centralized and federated identification models in Web 2.0 (OAuth 2.0, OpenID Connect): dependence on providers, concentration of leakage risks, and inability to disclose attributes selectively. The article reveals the mechanism of trust formation in the self-sovereign identity system, which is based on a three-party model of interaction between the issuer, the holder and the verifier; in this model, data authenticity is ensured using cryptographic verifiability through decentralized identifiers and verifiable credentials, which allows minimizing the participation of intermediaries, reducing the surface of possible attacks and guaranteeing the autonomy of the data subject in the process of managing their own digital identity. The key principles of self-sovereign identity (control, availability, transparency, minimization of disclosure, portability, security/resilience, and consent) are systematized, and their applied role in forming a «trust architecture» in Web3 (DAO, DeFi, NFT) is demonstrated. The study revealed a regulatory asymmetry between the technological development of self-sovereign identity systems and the level of their legal regulation. For Ukraine, key regulatory gaps have been specified that hinder the implementation of self-sovereign identity systems and limit the possibility of integrating Ukrainian e-government systems into the international Web3 space: the legislation lacks definitions of the terms «self-sovereign identity» and «decentralized identifier», which is why these concepts have no legal status in Ukraine; the current legal framework for electronic identification and personal data protection is incompatible with the principles of decentralization, self-control, and minimization of information disclosure, which underlie the SSI model. The practical significance of the results lies in the proposed holistic legal and technical framework for developing Web3 trust services, which enables the design of interoperable and secure processes for managing digital assets, prioritizing personal sovereignty over data.

Keywords: public control, authentication model, intermediary, personal data, regulatory support.

Самосуверенна ідентичність як основа управління цифровими активами у Web3 середовищі

Туголуков Олександр Євгенович,
головний комерційний директор, NOTA Digital Currencies Research Center Inc., 5307 Марконі авеню, м. Кармайкл, Каліфорнія. 95608, США,
https://orcid.org/0009-0008-3661-764X

Люшенко Дмитро Ігорович,
директор, NOTA LLC,
5307 Марконі авеню, м. Кармайкл, Каліфорнія. 95608, США,
https://orcid.org/0009-0003-9180-0934

Анотація. Стрімкий розвиток децентралізованих технологій та блокчейну трансформує способи автентифікації, управління даними й реалізації цифрових прав людини, що актуалізує потребу у формуванні нової парадигми ідентичності, заснованої на автономії користувача та довірчій взаємодії без посередників. Мета статті – обґрунтувати самосуверенну ідентичність як основу довіри та управління цифровими активами у Web3-екосистемі. Методологія дослідження поєднує порівняльно-правовий та формально-догматичний аналіз, структурно-функціональне моделювання тристоронньої взаємодії видавець – власник – перевіряючий, а також проблемно-орієнтований огляд технічних стандартів і практик ранніх платформ (Sovrin, uPort). Продемонстровано, що виникнення самосуверенної ідентичності є закономірною відповіддю на вади централізованих і федеративних моделей ідентифікації у Web 2.0 (OAuth 2.0, OpenID Connect): залежність від провайдерів, концентрація ризиків витоків, неможливість вибіркового розкриття атрибутів. У статті розкрито механізм формування довіри у системі самосуверенної ідентичності, який ґрунтується на

тристоронній моделі взаємодії між видавцем, власником та перевіряючим; у цій моделі достовірність даних забезпечується за допомогою криптографічної перевірюваності через децентралізовані ідентифікатори та перевірювані обліги, що дозволяє мінімізувати участь посередників, зменшити поверхню можливих атак і гарантувати автономність суб'єкта даних у процесі керування власною цифровою ідентичністю. Систематизовано ключові принципи SSI (контроль, доступність, прозорість, мінімізація розкриття, переносимість, безпека/стійкість, згода) і показано їхню прикладну роль для формування «архітектури довіри» у Web3 (DAO, DeFi, NFT). У ході дослідження виявлено наявність нормативної асиметрії між технологічним розвитком систем самосуверенної ідентичності та рівнем їх правового регулювання. Для України конкретизовано ключові нормативні прогалини, які стримують впровадження систем самосуверенної ідентичності та обмежують можливість інтеграції українських систем електронного врядування у міжнародний Web3-простір: у законодавстві відсутні визначення термінів «самосуверенна ідентичність» та «децентралізований ідентифікатор», через що ці поняття не мають юридичного статусу в Україні; чинні правові рамки електронної ідентифікації та захисту персональних даних є несумісними з принципами децентралізації, самоконтролю та мінімізації розкриття інформації, які лежать в основі моделі SSI. Практична значимість результатів полягає у запропонованій цілісній правово-технічній рамці для розвитку довірчих сервісів Web3, що дозволяє проєктувати інтероперабельні та безпечні процеси управління цифровими активами з пріоритетом персонального суверенітету над даними.

Ключові слова: публічний контроль, модель автентифікації, посередник, персональні дані, нормативне забезпечення.

Problem statement. The development of digital technologies, particularly blockchain, decentralized networks, and smart contracts, has given rise to a new paradigm of digital interaction – Web3 – which is based on decentralization, user

autonomy, and the elimination of intermediaries. In this context, the key challenge is the problem of identity verification in the digital environment, as traditional centralized authentication systems (through state or corporate registers, banking services, and social networks) have demonstrated their vulnerability to unauthorized access, leakage of personal data, and abuse by government or commercial entities. The concept of self-sovereign identity (SSI) presents a qualitatively different model, in which the user independently owns, controls, and disposes of their digital identifiers without intermediaries. This model serves as the foundation of trust in Web3 ecosystems, where transactions, digital asset management, and interactions between entities are facilitated through smart contracts and decentralized protocols. Despite the growing attention to the topic of SSI in the global scientific and technological community, several legal, managerial, and ethical aspects of its implementation remain unresolved. Firstly, there are no unified standards for the legal regulation of SSI in national jurisdictions, including Ukraine, which complicates the protection of digital assets, the recognition of electronic identifiers as legally significant, and the integration of decentralized identities into state electronic systems. In addition, the issues of the legal status of digital assets, their management through decentralized mechanisms (DAO, DeFi protocols, NFT platforms), as well as the balance between personal sovereignty and public control in the digital environment, are relevant. The insufficient development of the regulatory and organizational frameworks of SSI creates a threat of digital identity fragmentation, increased risks of fraud, money laundering, and a loss of trust in decentralized systems. Thus, there is a need for a comprehensive study of SSI as the foundation of digital asset management in the Web3 environment, which will enable the formation of a theoretical and legal basis for developing appropriate mechanisms for regulation, ensuring data security, and exercising the rights of subjects in digital relations within a new decentralized ecosystem.

Analysis of recent research and publications. In the scientific discourse of the last decade, a holistic theoretical and technological paradigm of SSI has emerged,

combining legal, technical, and socio-communication aspects of digital attribute management. Among the early conceptual explorations, a special place is occupied by the work of C. Allen [1], in which the principles of SSI were first formulated as a logical alternative to centralized authorization models. The author proposed fundamental provisions, including the priority of user control over their own identifiers, minimizing data disclosure, and ensuring the cryptographic integrity of their data. The technological implementation of SSI ideas in practice was analyzed by M. Lockwood [2], who proved that the construction of an accessible interface layer for SSI is a critical condition for the widespread implementation of the concept. The author showed that without convenient user solutions, the SSI system risks remaining an elitist technology limited to a circle of technical experts.

A significant contribution to the development of the technical architecture of SSI was made by C. S. Park and H. M. Nam [3], who proposed a new approach to building decentralized identifiers with the possibility of secure rotation of cryptographic keys. Their results have practical significance for increasing the resistance of SSI systems to key compromise and reducing the risks of unauthorized access. A significant theoretical contribution is made by the work of M. Kuperberg [4], which reviews identity management from the perspective of corporate ecosystems. The author found that the use of blockchain in identification systems has not only a technological but also an organizational effect: it contributes to the redistribution of trust from centralized authorities to network communities and reduces transaction costs in interorganizational processes. In the broader context of the digital transformation of enterprises, M. Dietz and G. Pernul [5] considered the concept of a «digital twin» as an infrastructure layer for decentralized interaction of systems. The authors concluded that the principles of data self-sovereignty and trustful interaction can be transferred from the individual to the corporate level, forming a «digital identity economy» in which enterprises act as equal participants in data exchange.

ISSN: 3041-2110

V. Savchenko and R. Maydanyk explored the legal aspects of the expression of will and individual autonomy in the digital environment [6] and the phenomenon of contracts implicitly based on the parties' will. They demonstrated that the modern legal field enables a transition from formalized to behavioral forms of consent, which has direct relevance for SSI models, where the user's expression of will confirms transactions through a digital signature or smart contract. J. Sedlmeir et al. [7] showed that the combination of Digital Identities and Verifiable Credentials forms a reproducible «trust machine» for interorganizational processes. The authors emphasize that the key value is not in the blockchain, but in the ability to separate the issuance of attributes from their verification without a permanent intermediary, which creates the basis for interoperable data markets.

For their part, A. Grüner et al. [8] proposed a general scheme of threats to self-sovereign identity systems and compared their resilience at different architectural levels. They proved that the most significant share of the risk is created not so much by algorithmic flaws as by «peripheral» components – wallets, key stores and recovery procedures – and this is where standardized mechanisms for secure rotational key management and countering social engineering are needed. At the intersection of technology and law, B. Custers, H. Ursic [9] outlined the limits of SSI compatibility with the General Data Protection Regulation (GDPR) regime, emphasizing that a decentralized approach in itself does not remove the issues of determining the «controller» and «processor» of data, the right to erasure and restriction of processing. Their conclusion is practical: for SSI not to conflict with the GDPR, the design should support data minimization, selective disclosure, and technically supported consent mechanisms, as well as clearly delineate the responsibilities of ecosystem participants. Finally, A. Mühle et al. [10] systematized the «mandatory components» of the SSI ecosystem. They showed that the viability of solutions is determined not by a single standard, but by the coordinated interaction of DID methods, cryptographic primitives, and trust policies.

Highlighting previously unresolved parts of the general problem. A generalization of the literature suggests that despite the intensive development of the technical and organizational aspects of SSI, the problem of legal unification and institutional consolidation of the SSI principle remains unresolved. The mechanisms for integrating decentralized identifiers into state electronic identification systems, as well as the issue of mutual recognition of SSI attributes between jurisdictions, remain insufficiently developed. It is these gaps that determine the relevance of the research conducted, which aims to combine the legal, technological, and ethical dimensions of digital asset management in the Web3 environment.

Formulation of the article objectives (task statement). The purpose of the article is to substantiate the theoretical and legal foundations of the formation and application of SSI in the Web3 environment as a tool for ensuring safe and transparent management of digital assets. To achieve this goal, the article sets the following tasks: to reveal the essence and fundamental principles of SSI and its role in establishing trust between participants in the Web3 ecosystem; to identify problematic aspects of the legal regulation of SSI and digital assets at both the international and national levels, particularly in Ukraine.

Presentation of the main research material. The formation of the SSI concept is linked to a shift in the understanding of digital identification that occurred in the 2010s, in response to the limitations of centralized and federated identity management models. In the Web 2.0 paradigm, authentication relied on an authorization and access delegation infrastructure, in particular the OAuth 2.0 protocol and the OpenID Connect add-on, which standardized the interaction of clients with authorization servers and allowed identity providers (large platforms such as Google or Facebook) to be actual gateways to access third-party services and user data. Despite significant achievements in unifying authorization flows, this model perpetuates the structural dependence of the user on the service provider, increases the risks of aggregated leaks, and recreates the asymmetry of control over personal attributes. That is why, since 2016, a discussion has been underway in the

scientific and technical community about the need to return control over identity directly to its bearer. A key intellectual event was the programmatic essay by K. Allen, «The Path to Self-Sovereign Identity», which proposed the principles of SSI as a new concept of trust on the Internet, with a focus on user ownership of identifiers, minimizing disclosure and portability of attributes between systems [1].

The idea was further developed through the institutionalization of work at W3C and the formation of an engineering ecosystem around the Decentralized Identity Foundation (DIF). It was within the W3C that the technological basis of SSI was laid: first, through the Decentralized Identifiers (DID) v1.0 specification, which on July 19, 2022 acquired the status of a W3C Recommendation, which means readiness for widespread implementation and inter-agency interoperability [11]; second, through the updated Verifiable Credentials (VC) Data Model v2.0, approved as Verifiable Credentials Data Model v2.0 – W3C Recommendation [12] and supplemented by a family of cryptographic design documents (VC-JOSE-COSE, SD-JWT, etc.). The participation of the DIF, as an engineering-oriented consortium, ensured the development of open components, interoperability testing, and agreement on approaches between the business and the developer community.

In parallel, the SSI concept was developed in experimental and production networks. One of the early platforms was the Sovrin ecosystem, which offered a public distributed infrastructure [13]. This initiative, along with several projects on open networks (particularly uPort on Ethereum), has transformed SSI from a theoretical framework into a practical identity management toolkit suitable for applications in areas such as access, regulatory compliance, education, healthcare, and government services. It was the operational experience of early platforms that demonstrated that decentralized identifiers and verifiable attributes could reduce the attack surface, provide consent control, and increase verifiability without storing personal data in centralized repositories.

In the scientific and regulatory discourse, SSI has been positioned from the beginning as a direct response to the systemic limitations of the centralized-federated

model. While OAuth 2.0 and OpenID Connect have historically provided scalable authorization and unified authentication for the Web ecosystem, their logic of trust – through the identity provider – makes the user dependent on the policies and technical failures of the intermediary, and also complicates the selectivity of attribute disclosure and cryptographic provability with a minimum of data. Instead, SSI shifts the center of trust to the subject and reduces the intermediary functions to attribute publishers and verifiers, who do not need to maintain complete profiles or centralized databases. The transition from identification as a «platform service» to identity as a «subject property», supported by W3C open web standards, is the historical novelty of SSI.

The SSI architecture is based on a three-party model of interaction between the issuer, the holder, and the verifier. This structure ensures user autonomy and eliminates the need for centralized intermediaries.

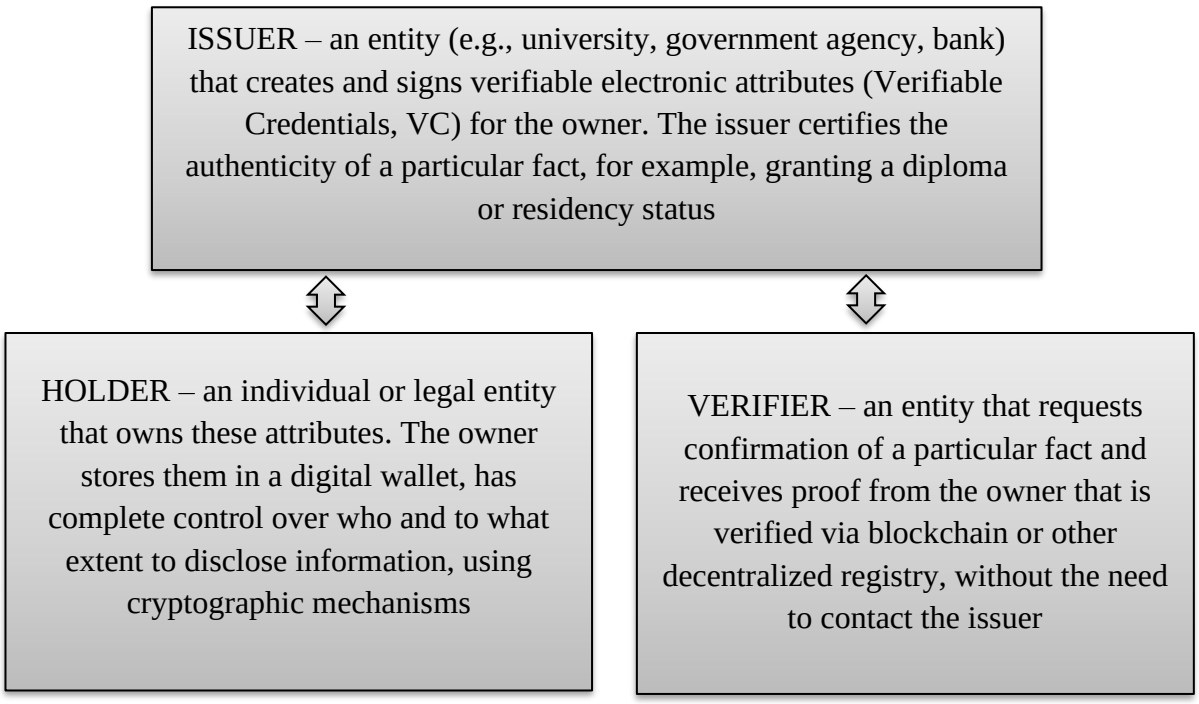

Fig. 1. SSI structure

Source: compiled by the authors based on [14]

The interaction mechanism is built on the principle of cryptographic verifiability: each VC contains a digital signature of the publisher, which the verifier can verify via DID – a decentralized identifier registered in the blockchain. This model eliminates the constant participation of the publisher, ensuring the autonomy of processes and minimizing the risks of personal data leakage. Table 1 summarizes the principles of SSI.

Table 1

Basic principles of SSI

Principle	Content	Practical significance in the Web3 ecosystem
Control	The user wholly owns, controls and revokes their own digital identifiers and attributes	Ensures personal sovereignty over identity; eliminates dependence on state or corporate providers
Access	The individual has constant access to their data regardless of location, time or technical platforms	Guarantees continuity of identification across different decentralized applications (dApps)
Transparency	SSI protocols and algorithms are open for community verification and audit	Increases the level of trust and compliance with international security standards (ISO/IEC 29100)
Minimal disclosure	Only the amount of information necessary for a specific transaction is transmitted	Implements the principle of privacy by design; reduces the risk of unauthorized access
Portability	Identifiers and attributes can be used in any compatible Web3 environment	Ensures interoperability between different blockchain networks and platforms
Security and Persistence	Identifiers are cryptographically protected; they cannot be changed or destroyed without the owner's consent	Guarantees long-term validity; eliminates centralized points of failure
Consent	Any use of identifiers or attributes is only made after the owner's voluntary consent	Compliant with GDPR and the principle of self-determination of the person in the digital space

Source: compiled by the authors based on [7; 8]

The table below systematizes the key principles of SSI, which form a holistic ethical, technical and legal framework for the functioning of decentralized systems in the Web3 environment. Taken together, these principles define not only the technological architecture, but also a new philosophy of trust based on user autonomy, process transparency and cryptographic provability. However, the

development of SSI technologies has a significant gap with the regulatory and legal field: technological progress significantly outpaces the formation of adequate legal frameworks, which creates a regulatory asymmetry between the capabilities of systems and their regulation. On the one hand, SSI aims to grant users complete control over their own digital identities [9]. On the other hand, the legal systems of many jurisdictions do not contain an agreed-upon definition of SSI, clear rules for its application, and do not cover all new technological models, particularly tokenized attributes and decentralized identifiers. In the European Union, the concept of SSI is primarily interpreted through the lens of the eIDAS 2.0 regulation as a component of the European Digital Identity Wallet – a digital wallet where a citizen independently stores and controls their attributes issued by official bodies [15]. In this approach, SSI is viewed not as a complete rejection of centralized regulation, but as a «user-centric model under institutional trust» – a model where the user owns their data, but the state remains the guarantor of their authenticity and legal recognition. In the United States of America, there is no single regulatory definition of SSI. Still, several strategic documents (in particular, the National Strategy for Trusted Identities in Cyberspace) consider it as a «decentralized, blockchain-enabled identity framework» that ensures private control and voluntary disclosure of information [16]. The American approach emphasizes market self-regulation and flexibility – SSI is viewed primarily as an innovative technological architecture, and not as a subject of direct state regulation. The lack of a unified international definition of the concept of SSI and its legal status in this context poses a significant obstacle to law enforcement and international interoperability.

Additionally, significant differences are emerging between regulatory approaches in various jurisdictions. In the European Union (EU), electronic identification frameworks are being actively developed (in particular, the eIDAS regulation and adaptation to decentralized models), aimed at integration into an interoperable trust system at the EU level. In the US, approaches remain more decentralized, stimulating private-market initiatives, but do not establish a single

federal standard for digital identity. In Asia and the post-Soviet space, state-oriented electronic identification systems predominate, often failing to account for user autonomy and decentralization. Such regional differences create difficulties with cross-border interaction, trust between systems, and compatibility of approaches [10].

In Ukraine, there is currently no clear legislative definition of the concepts of SSI or decentralized identifier. No regulatory legal act contains such terms as separate legal categories, which creates a space of legal uncertainty and complicates the implementation of SSI models in both the public and private sectors. The sphere of electronic identification and electronic trust services in Ukraine is regulated, in particular, by the Law of Ukraine «On Electronic Identification and Electronic Trust Services» № 2155-VIII [17]. This regulatory act is based on the model of the European Regulation (EU) № 910/2014 (eIDAS) [18] and focuses on centralized and federated identification, which is achieved through trust service providers, certification of electronic signatures, and other centralized mechanisms. At the same time, it does not provide mechanisms for decentralized control by the user of their own identity or attributes, which are fundamental to the SSI model.

Another regulatory focus is the Law of Ukraine «On Personal Data Protection» № 2297-VI [19], which regulates the protection of personal data. Still, it does not provide for the exclusive transfer of data and control over them by the owner in the form characteristic of the SSI model (when the subject independently manages its attributes, grants permission for their use, distributes only what is necessary, and transfers the identifier between systems). Thus, the legislative framework is not well-suited for implementing the principles of minimizing disclosure, portability, and self-control, which are characteristic of SSI. Regarding the legal regime of digital assets, the situation also remains problematic. Ukraine adopted the Law of Ukraine «On Virtual Assets» № 2074-ИХ [20]. This law creates a legal framework for the circulation of virtual assets. Still, it has not yet entered into force as of today (due to the failure to approve the relevant bylaws and taxation

mechanisms). It creates significant regulatory gaps: there are no clear rules for registering virtual asset service providers, a system of control, taxation, or mechanisms for protecting users' rights, or liability limits. Combined with the lack of a regulatory framework for SSI, this limits the possibilities for integrating digital assets with decentralized identity.

It is also important to emphasize that the interaction of Ukrainian state electronic systems, particularly the «Diia» platform, with SSI models remains at the conceptual level. To date, there are no implemented pilot projects that would use decentralized identifiers or blockchain infrastructure in the public sector. Potential areas for implementing such solutions could be education, healthcare, financial services, or social services, but these opportunities remain unrealized. There is also a lack of an agreed regulatory framework, technical standards and a state strategy that would ensure the practical integration of SSI approaches into national information systems. In the absence of a legally approved methodology for interaction between such systems and the user, as well as standardized mechanisms for transferring attributes and identifiers between registered partners, the implementation of the SSI approach remains limited.

As a result of the analysis, the Ukrainian legal framework in the field of digital identity and digital asset management has a set of systemic problems that significantly complicate the implementation of SSI in practice. First, there is no legal recognition of SSI as a digital identity model in Ukraine. No current law or bylaw contains a definition of the concepts of self-sovereign identity or decentralized identifier, which makes their official use in legal and administrative procedures impossible. Such a regulatory gap creates uncertainty regarding the status of SSI ecosystem entities (publishers, owners, verifiers), their rights and obligations, as well as the limits of liability in cases of security breaches or unauthorized access to data. As a result, technological initiatives to implement SSI remain outside the legal framework and cannot be legally integrated into state electronic services. Secondly, there is a lack of compliance of current legislation with the principles of

decentralization, self-control, and data portability. The norms of the Law of Ukraine «On Electronic Identification and Electronic Trust Services» [17] and the Law of Ukraine «On Personal Data Protection» [19] are built on a centralized logic of identity management, where state or certified providers perform key functions. Such a model contradicts the essence of SSI, in which the user should be the owner and manager of their digital attributes. The lack of mechanisms for independent control over identifiers, as well as the legal possibility of transferring them between different systems, limits the implementation of an individual's right to digital sovereignty and self-determination in cyberspace.

Third, the digital asset market remains unregulated, which directly affects the implementation of SSI as an infrastructure element of the Web3 economy. Although the Law of Ukraine «On Virtual Assets» (2022) has been adopted, it has not yet entered into force due to the lack of by-laws, taxation mechanisms and supervisory authorities. As a result, Ukraine lacks a legal framework for identifying token owners, conducting transactions with digital assets and verifying them through SSI mechanisms. This situation creates risks of legal conflict between economic activity in the field of crypto assets and the principles of digital trust implemented by SSI. These circumstances create a regulatory vacuum that significantly complicates the implementation of SSI models and the associated digital asset management infrastructure in Ukraine.

Conclusions. Thus, the formation of the SSI concept has become a natural reaction to the limitations of centralized and federated digital identification systems. Traditional authentication models built on the OAuth 2.0 and OpenID Connect protocols, while ensuring scalability, also created user dependence on identity providers and trust intermediaries. Instead, SSI proposed a different logic – transferring control over digital identity to the user themselves.

A regulatory asymmetry was identified between the development of SSI technologies and the state of their legal regulation. International approaches form only general guidelines, without defining a clear legal status of decentralized

identity. In the EU, SSI is integrated into the framework of institutional trust through the European Digital Identity Wallet. In the USA, private-market models, lacking a single regulatory framework, dominate. In post-Soviet states, a state-centric approach prevails.

In Ukraine, legal regulation of digital assets remains fragmented. The laws «On Electronic Identification and Electronic Trust Services» and «On Personal Data Protection» are focused on centralized authentication systems and do not take into account the principles of self-control and decentralization. The law «On Virtual Assets» has not yet been put into effect, and the lack of a state strategy for SSI and pilot blockchain projects (in particular, within the framework of the «Diia» platform) deepens the regulatory vacuum. Thus, SSI is not only a technological innovation, but also a socio-legal innovation that requires coordination with European standards, such as eIDAS 2.0 and MiCA, the determination of the legal status of decentralized identifiers, and the practical implementation of SSI projects in the public sector. It will serve as the foundation for a safe, trustworthy, and interoperable digital space in Ukraine, where citizens will have genuine control over their identity and assets.

References

1. Allen C. The path to self-sovereign identity. *Life With Alacrity Design Patterns for Digital Collaboration & Trust*. 2016. URL: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity (access date: 22.08.2025).

2. Lockwood M. An accessible interface layer for self-sovereign identity. *Frontiers in Blockchain.* 2021. Vol. 3. 609101. DOI: https://doi.org/10.3389/fbloc.2020.609101.

3. Park C. S., Nam H. M. A new approach to constructing decentralized identifier for secure and flexible key rotation. *IEEE Internet of Things Journal*. 2021. Vol. 9, № 13. P. 10610-10624. DOI: https://doi.org/10.1109/JIOT.2021.3121722

4. Kuperberg M. Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. *IEEE Transactions on Engineering Management.* 2020. Vol. 67, № 4. P. 1008–1027. DOI: https://doi.org/10.1109/TEM.2019.2926471.

5. Dietz M., Pernul G. Digital twin: empowering enterprises towards a system-of-systems approach. *Business & Information Systems Engineering*. 2020. Vol. 62. P. 179–184. DOI: https://doi.org/10.1007/s12599-019-00624-0.

6. Savchenko V., Maydanyk R. Contracts implied-in-fact like a form of will expression. *Access to Justice in Eastern Europe*. 2024. Vol. 7, № 2. P. 283-300. DOI: https://doi.org/10.33327/AJEE18-7.2-a000212.

7. Sedlmeir J., Smethurst R., Rieger A., Fridgen G. Digital identities and verifiable credentials. *Business & Information Systems Engineering*. 2021. Vol. 63, № 5. P. 603–13. DOI: https://doi.org/10.1007/s12599-021-00722-y.

8. Grüner A., Mühle A., Lockenvitz N. Analyzing and comparing the security of self-sovereign identity management systems through threat modeling. *International Journal of Information Security*. 2023. Vol. 22. P. 1231–1248. DOI: https://doi.org/10.1007/s10207-023-00688-w.

9. Custers B., Ursic H. Can self-sovereign identity (SSI) fit within the GDPR? *CiTiP Blog, KU Leuven*, 2023. URL: https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-fit-within-the-gdpr-part-i/ (access date: 22.10.2025).

10. Mühle A., Grüner A., Gayvoronskaya T., Meinel C. A survey on essential components of a self-sovereign identity. *Computer Science Review*. 2018. Vol. 30. P. 80–86. DOI: https://doi.org/10.1016/j.cosrev.2018.10.002.

11. Decentralized Identifiers (DIDs) v1.0. *W3C Recommendation 19 July 2022*. URL: https://www.w3.org/TR/did-1.0/ (access date: 22.10.2025).

12. W3C. Verifiable Credentials Data Model v2.0 – W3C Recommendation (15.05.2025). URL: https://www.w3.org/TR/vc-data-model-2.0/ (access date: 22.08.2025).

13. Sovrin Foundation. Sovrin: A Protocol and Token for Self-Sovereign Identity & Decentralized Trust. URL: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf (access date: 22.08.2025).

14. Schardong F., Custódio R. Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*. 2022. Vol. 22, № 15. 5641. DOI: https://doi.org/10.3390/s22155641

15. EU A digital ID and personal digital wallet for EU citizens, residents and businesses. *European Commission*. URL: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU%2BDigital%2BIdentity%2BWallet%2BHome (access date: 22.08.2025).

16. National Strategy for Trusted Identities in Cyberspace (NSTIC). *NIST*. URL: https://www.nist.gov/blogs/cybersecurity-insights/get-involved-national-strategy-trusted-identities-cyberspace-nstic (access date: 22.08.2025).

17. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/2155-19 (access date: 22.08.2025).

18. Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). *Official Journal of the European Union*, L 257/73. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R091 (access date: 22.08.2025).

19. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (access date: 22.08.2025).

20. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2074-20 (access date: 22.08.2025).