Administrative Law and Procedure

UDC 347.77/.78:004.738.5

DOI https://doi.org/10.5281/zenodo.17598639

Digital identity tokenization as a challenge to traditional legal concepts of property

Nodari Gorgiladze,

Program Director, NOTA Digital Currencies Research Center Inc.,

Sacramento, California, USA, https://orcid.org/0009-0007-2384-0036

Accepted: 27.10.2025 | Published: 13.11.2025

Abstract. In the context of the spread of blockchain technologies and the emergence of the digital economy, a profound transformation of legal concepts related to property, personal data, and identity is underway. The tokenization of a person's digital attributes creates a new paradigm of legal relations among the user, the state, and digital platforms, within which the line between private control and legal ownership becomes blurred. The relevance of the topic stems from the lack of a unified legal approach to identity tokens as objects of property rights and personal rights, which creates risks of legal uncertainty in the digital environment. The purpose of this article is to provide a theoretical and legal understanding of the phenomenon of tokenization of digital identity and to determine its impact on traditional concepts of property rights. The paper employs comparative legal, systemic, and structural, as well as analytical and formal legal methods. The comparative analysis covered the practices of the European Union, the United States, Ukraine, and Singapore. Empirical materials from eIDAS 2.0, GDPR, UCC-2022, and PDPA were used to identify standard and distinctive features. It was found that tokenization of digital identity combines elements of personal data, intellectual

property, and digital assets, generating legal uncertainty regarding its status. In all the jurisdictions studied, the digital identity token is not recognized as an object of full ownership; instead, it is treated as a carrier of personal control rights. The concept of «digital ownership» is proposed – a new legal institution that allows the user to exercise control over the token without losing personal sovereignty. The need to harmonize technical standards (W3C VC 2.0, DID) with the legal frameworks of eIDAS 2.0 and national laws, as well as the creation of cross-border mechanisms for recognizing tokenized identifiers, is substantiated. The results obtained can be used to develop a national concept of digital identity for Ukraine, improve legislation in the field of electronic trust services and personal data protection, as well as contribute to the formation of international standards for digital ownership and cross-border legal cooperation in the field of digital identification.

Keywords: blockchain technology, personal data, legal relations, user, state.

Токенізація цифрової ідентичності як виклик для традиційних правових концепцій власності

Горгіладзе Нодарі Русланович,
директор програми, NOTA Digital Currencies Research Center Inc.,
м. Сакраменто, Каліфорнія, США, https://orcid.org/0009-0007-2384-0036

Анотація. У контексті поширення технологій блокчейну та формування цифрової економіки відбувається глибинна трансформація правових уявлень про власність, персональні дані та ідентичність. Токенізація цифрових атрибутів особи створює нову парадигму правовідносин між користувачем, державою й цифровими платформами, у межах якої межа між приватним контролем і юридичним володінням стає розмитою. Актуальність теми зумовлена відсутністю уніфікованого правового підходу до токенів ідентичності як об’єктів прав власності та персональних прав, що породжує

ризики правової невизначеності у цифровому середовищі. Мета статті полягає у теоретико-правовому осмисленні феномену токенізації цифрової ідентичності та визначенні її впливу на традиційні концепції права власності. У роботі застосовано порівняльно-правовий, системно-структурний, аналітичний та формально-юридичний методи. Порівняльний аналіз охопив практику Європейського Союзу, США, України та Сінгапуру. Для виявлення спільних і відмінних рис використано емпіричні матеріали eIDAS 2.0, GDPR, UCC-2022, Personal Data Protection Act (PDPA). Встановлено, що токенізація цифрової ідентичності поєднує елементи персональних даних, інтелектуальної власності та цифрового активу, породжуючи юридичну невизначеність щодо її статусу. У всіх досліджених юрисдикціях токен цифрової ідентичності не визнається об'єктом повного права власності, натомість трактується як носій персональних прав контролю. Запропоновано концепцію «цифрового володіння» – нового правового інституту, який дозволяє користувачу здійснювати контроль над токеном без втрати персонального суверенітету. Обґрунтовано необхідність гармонізації технічних стандартів (W3C VC 2.0, DID) із правовими режимами eIDAS 2.0 та національних актів, а також створення транскордонних механізмів визнання токенізованих ідентифікаторів. Отримані результати можуть бути використані для розроблення національної концепції цифрової ідентичності України, вдосконалення законодавства у сфері електронних довірчих послуг і захисту персональних даних, а також при формуванні міжнародних стандартів цифрового володіння та транскордонного правового співробітництва у сфері цифрової ідентифікації.

Ключові слова: технології блокчейну, персональні дані, правовідносини, користувач, держава.

Problem statement. The rapid development of the digital economy and blockchain technologies is changing the perception of ownership, control and

personal identity in the digital environment. The concept of tokenization, initially applied to financial instruments and crypto-assets, is now being extended to personal data, digital profiles, and elements of user identity. In this context, digital identity is transformed from a set of information attributes into an economically significant asset that can be owned, transferred or even traded in the form of tokens. However, such a transformation raises questions about the traditional legal concepts of property, which were developed within the framework of property and contract law. In particular, the question arises: can digital identity be considered as an object of property rights, or does it belong to the category of personal non-property rights that are inalienable by their nature? Legal doctrine has not yet developed a unified approach to the nature of tokenized assets, and even more so to «identity tokens», which combine features of personal data, intellectual property, and digital code.

The problem is complicated by the fact that modern digital identification mechanisms (in particular, self-sovereign identity (SSI), decentralized identifiers (DID), verifiable credentials (VC)) involve delegating control over one's own digital attributes to the user without apparent legal certainty regarding the legal status of such data. That is, there is a gap between the user's technological autonomy and legal regulation, which remains within the framework of classical property models developed for material objects.

Analysis of recent research and publications. Analysis of scientific works reveals that the phenomenon of digital identity tokenization is regarded in modern literature as an interdisciplinary concept that encompasses legal, technological, and socio-economic aspects of data management. In their work, A. Boysen [1] emphasizes that the evolution of digital identification systems from centralized models to self-sovereign ones is a natural response to the crisis of trust in state and corporate intermediaries. The author found that the decentralized model provides a greater level of user autonomy and reduces the risk of unauthorized access to personal data, while creating a need for new legal mechanisms to ensure responsibility for the preservation of digital attributes. The study by R. M. Garcia-

Teruel and H. Simón-Moreno [2] concluded that the process of digital tokenization alters the legal nature of property ownership. Instead of the traditional title of ownership, a dynamic system of control over the digital asset is established. The authors demonstrate that, in most jurisdictions, tokenized rights lack a stable property status, which leads to conflicts when determining the parties' competence and the limits of their responsibility upon transferring such tokens. G. Wang and M. Nixon [3] proposed a systematization of tokenization forms in blockchain ecosystems, distinguishing between three types of tokens: information, financial, and identification. They demonstrated that identification tokens serve a unique function - they not only represent data but also confirm subjectivity in the digital environment. The authors emphasized that tokenization in this area creates the prerequisites for a new level of digital interaction, but requires legal regulation of the conditions of access and management of tokens.

S. Joshi and A. Choudhury's research [4] demonstrated that tokenization technology can transform asset management in high-capitalization sectors, such as real estate. The authors demonstrated that transforming ownership rights into tokens enhances transparency and market accessibility, but simultaneously creates risks of dual ownership and necessitates new standards for digital control. Their findings are relevant for the tokenization of digital identity, where a similar problem arises in connection with the transfer of rights to identification attributes. On the technical side, L. Kaptosv [5] investigated how the use of Redis technologies optimizes caching in high-load web applications. The author concluded that effective management of database queries and reduction of system response time directly affect the stability of digital identity platforms. Therefore, the technical architecture of tokenized systems also becomes a factor in the legal reliability of their operations. H. Al-Ababneh et al. [6] found that big data analysis can effectively detect economic abuse in public procurement. This approach demonstrates the potential of algorithmic control over digital transactions, which can be applied to tokenized identification systems to monitor their integrity and protect against fraud. L. Lee [7]

revealed that the recognition of digital assets as objects of property differs significantly between legal systems. The author found that in several countries, a digital asset is considered a «controlled record» and not as a thing that can be the subject of classical property. It suggests that digital identity tokens should be attributed not to property, but to the personal rights of the user.

A significant contribution to the understanding of the legal nature of digital identity was made by A. Sharif et al. [8], who analyzed the evolution of the eIDAS regulation and the development trends of European electronic identification schemes. They demonstrated that the current EU policy is centered on establishing a unified digital infrastructure that relies on mutual recognition of identities and empowers users to control their own data.

The study by J. Kreppmeier et al. [9] expands the understanding of the economic logic of tokenization, showing that market mechanisms for trading tokenized assets (in particular, in the real estate sector) depend not only on regulatory factors, but also on the behavioral expectations of users. The authors emphasize that the transition to tokenized forms of ownership requires not only technological transparency but also legal stability of operations, which is related to the issue of protecting the rights of owners of digital identifiers. A similar line is developed by R. Ebadi [10], who proves that successful tokenization of assets is possible only if the token is legally recognized as a carrier of property rights. The author formulates the concept of «tokenized title», which can also be applied to the sphere of digital identity.

Highlighting previously unresolved parts of the general problem. Previous studies show that the tokenization of digital identity is a multidimensional process in which technical innovations significantly outpace legal doctrine. Despite achievements in standardizing technical solutions and developing self-sovereign models, the issues related to the legal nature of tokenized personal attributes and the limitations of their alienability remain unresolved. It is these gaps that are the object of further research within the framework of this article.

Formulation of the article objectives (statement of the task). The article aims to reveal legal conflicts and theoretical contradictions that arise as a result of the tokenization of digital identity. To achieve the set goal, the following research tasks are envisaged: to clarify the essence of the tokenization of digital identity and its technical and legal features; to analyze existing approaches of international law to the regulation of digital identifiers and tokenized personal data; to identify gaps in the national legal framework regarding the definition of the legal status of tokenized identity and the possibilities of its legal protection.

Presentation of the main material of the study. In the modern digital environment, the concept of «tokenization» acquires special significance as a technological and legal phenomenon of transforming information or intangible assets into digital tokens that can be stored, transferred and confirmed using distributed ledgers. In the classical sense, tokenization was primarily considered in the field of data security, for example, replacing confidential information with a substitute token that has no intrinsic value but allows processing without disclosing the original [3]. However, with the spread of blockchain technologies, smart contracts, and digital assets, the tokenization model has significantly expanded its meaning: a digital token is not just a protection or substitute for data, but a new way of expressing rights, control, and interaction in the digital space. In this context, tokenization means the process by which an intangible asset – for example, personal data, digital identity attributes or access rights – is converted into a token (or set of tokens) in a distributed ledger (table 1). This token can be verified, transferred, stored and, if necessary, subject to programmable interaction (via smart contracts) [4]. Thus, the token performs a dual function: it is a digital representative of the asset, as well as a carrier of a legal or functional mechanism for its use, control or transfer. For example, in the field of finance, asset tokenization involves representing real estate and securities in the form of tokens. If this approach is transferred to the sphere of digital identity, then in this case, tokenization means giving identity attributes a new «formula of existence» in the digital space – they

can be expressed as a token controlled by the user, verified using cryptography, and subjected to legal interpretation as an asset, resource, or component of the digital self.

Table 1

The difference between the classical and modern understanding of tokenization

Comparison criterion	Classical understanding of tokenization	Digital identity tokenization
Initial goal	Maintaining the security of confidential data by substituting it in processing processes	Giving the user cryptographically verifiable control over their own digital attributes
Object of tokenization	Bank card number, personal or payment data, confidential information	Digital identity attributes: name, electronic signature, biometrics, cryptographic keys, access rights
Technological basis	Centralized databases, token servers, and substitution algorithms	Distributed registries (blockchain), smart contracts, DID, W3C VC
User control level	Limited - control is exercised by the organization or payment provider	Full - the user owns and manages access to its tokenized attributes
Legal nature	Technical means of data protection do not have an independent legal status	Hybrid legal object, combining features of personal data, intangible asset and identification tool
Risks and challenges	Unauthorized access, token compromise, database security breach	Legal uncertainty of token status, jurisdictional conflicts, and violation of personal sovereignty over data
Role in the digital economy	Cybersecurity and transaction protection tool	Elements of digital citizenship, self-identification mechanism and trust management

Source: compiled by the author based on [1; 3; 4]

Comparative analysis reveals that digital identity tokenization represents a qualitatively new stage in the evolution of the tokenization concept, surpassing the traditional understanding of it as a technological tool for data protection. If in the classical paradigm a token is only a substitute for confidential information without independent value, then in the modern model it turns into a legal and functional carrier of the user's digital self.

In a general sense, digital identity refers to a set of attributes, data, accounts, cryptographic keys, and other elements that enable the identification of a person (or

organization) in the digital environment, verify this identity, and manage access to services or data based on it [11]. These attributes may include: name (or pseudonym), date of birth, biometric data, cryptographic keys, registration records, certificates, and accounts in various online services, among others. Importantly, digital identity is not limited to formal proof of identity (such as a passport), but encompasses digital footprints, online presence, reputation data, connections, behavioral metadata, and other relevant information. A new approach to digital identity management is emerging, known as SSI. It is based on the idea that a user owns, controls, and manages their digital attributes without the need for constant mediation by a centralized third party.

One of the key technological foundations of SSI is the use of DIDs, which enable the creation of unique, persistent, and cryptographically verifiable identifiers without relying on a centralized registry [12]. The combination of tokenization and the SSI concept enable us to discuss digital identity tokenization as the process of granting a user cryptographically verifiable control over their own digital attributes. In other words, digital identity becomes not just a set of data or attributes, but a digital asset – a token that a user can own, manage, grant or restrict access to, and so on. This approach opens up new possibilities for authentication, authorization, and digital interaction, but at the same time raises complex legal questions regarding the nature of these tokens, their status, and the legal consequences of ownership and transfer. For example, is a digital identity token an object of property rights or only a right to use; what guarantees should exist to protect such a token; can it be transferred to another person; how are the risks of losing control over it, changing the token, or interference by third parties taken into account.

In the context of digital identity tokenization, it becomes clear that this phenomenon extends beyond a mere technical solution and touches on three interconnected legal planes: personal data, intellectual property, and digital assets. Therefore, a digital identity token forms a hybrid legal object that encompasses the characteristics of: personal data (sensitivity, privacy, protection), intellectual

property (control, rights of use, possible alienability) and a digital asset (storage, transfer, economic function). This combination generates legal uncertainty. On the one hand, a token containing a digital identity or its attributes can be considered an asset that belongs to the user – they have control, can transfer or grant access, disable, or change it. But classic concepts of property rights – developed for tangible things or objects that physically exist – do not apply to «digital identity tokens». In Western legal doctrine, the question of «whether a digital asset is property» has already been explored: the authors insist that the legal status of digital assets varies significantly between jurisdictions [7]. In the case of an identity token, this issue becomes even more complicated: after all, it is not so much «property» in the usual sense, but rather a tool for implementing identity, controlling data, and confirming the subject, which is more reminiscent of a personal non-property right. For example, control over one's own data in the context of the General Data Protection Regulation 2016/679 (GDPR) [13] is precisely a personal right – the subject's right to access, rectify, delete, etc. – and not a traditional property right. The lack of a well-established approach creates legal uncertainty, which can lead to contentious situations.

Additionally, the issue of jurisdictional definition is also noticeable (table 2). The token is created in a global blockchain environment, where technology knows no borders, but legal regulation is tied to states, their legislation and jurisdiction.

Table 2

Comparative analysis of the legal status of digital identity tokens in selected jurisdictions (EU, US, Ukraine, Singapore)

Jurisdiction	Basic acts	Is «ownership» of an identity token recognized	Personal data regime for the token
EU	Regulation (EU) 2024/1183 (eIDAS 2.0), implementing acts and reference standards; compatibility with W3C VC 2.0 specifications	No, focus on data subject rights and trust services; «ownership of data» is not fixed	GDPR defines subject rights (access, erasure, etc.); processing of attribute tokens is subject to principles of law

Jurisdiction	Basic acts	Is «ownership» of an identity token recognized	Personal data regime for the token
US	NIST SP 800-63-4 (technical guidance); CCPA/CPRA and CPPA (California) rules, state laws, etc.; UCC-2022 (art. 12 on CER)	Partly through UCC-art. 12: «control» as an analogue of possession in relation to controlled electronic records; «identification token» not directly typified	Sectoral approach; in California, extended consumer rights, but not «ownership of data»
Ukraine	Law No. 2155-VIII «On Electronic Trust Services»; official clarifications on «Actions»	No, model tends towards eIDAS: tokens/digital documents – tools of identification/trust services, not «property»	Personal data regime identical to the European approach (subject rights, legality of processing)
Singapore	PDPA (amendments 2020–2021); NDI/Singpass; IMDA/GovTech initiatives on VC/DID (sgDID, TrustVC, SingVC) based on W3C	No; focus on lawful processing/consent and trusted issuance/verification infrastructure	Strict PDPA regime: integrity, purpose limitation, security, access and correction

Source: formed by the author based on [13-22]

For example, at the EU level, Regulation (EU) No. 910/2014 (eIDAS Regulation) [14] on electronic identification and trust services is in force, providing standards for the mutual recognition of identification schemes. At the same time, personal data protection rules, such as the GDPR, regulate the processing of data subjects. In the USA, Singapore and other countries, there are different approaches to digital identification systems, asset tokenization and their legal status. Therefore, a user who owns an identity token can be subject to the laws of multiple jurisdictions. The technological record exists globally, but the legal recognition or protection of this record depends on the specific legal system. The lack of a unified legal system creates risks: for example, a token may lose its legal force in one country but remain valid in another, or the state may not recognize the transfer of such a token as legally valid.

The comparative analysis shows that none of the jurisdictions considered has yet formed a full-fledged legal regime of «ownership» of digital identity tokens. In all cases, the prevailing approach is that digital identity and its associated tokens are

considered primarily as carriers of personal data and authentication tools, rather than as independent objects of property rights. The European model (eIDAS 2.0 + GDPR) prioritizes the rights of the data subject and trust mechanisms, making the commercialization of identity impossible, while providing a high level of legal certainty and cross-border compatibility. The American system, on the contrary, demonstrates fragmentation and pragmatism. Within the framework of UCC-2022 (Art. 12), the concept of a «controlled electronic record» is introduced, which partially brings the token closer to the property category; however, the absence of a federal law on digital identity preserves regulatory uncertainty. Ukraine is consistently harmonizing its national regulatory framework with the European one, focusing on the principles of eIDAS, as confirmed by the development of the «Diia» infrastructure as a national digital wallet. However, the legal doctrine does not yet contain a definition of the legal status of tokenized personal attributes. Singapore, in turn, demonstrates a state-centric approach that combines centralized identification (Singpass) with elements of decentralized verified identities (VC/DID), ensuring a balance between innovation and control over the processing of personal data under the PDPA.

In general, the trend of global development is the gradual convergence of technical and legal standards for tokenized identity. The European model provides legal integration, the American model provides market flexibility, the Ukrainian model provides harmonization, and the Singapore model provides managerial stability. At the same time, a key gap remains the lack of a precise legal categorization of identity tokens as objects of property rights, which requires the development of new concepts of digital ownership and personal sovereignty over data. The development of tokenized digital identity models requires the creation of a legal architecture capable of ensuring a balance between the user's technological autonomy, the right to privacy, and the fundamental principles of property and legal control. The first step should be to normatively consolidate the legal status of a digital identity token as a special type of intangible asset that combines the features

of personal data and a digital record, but is not an object of complete alienation. It is advisable to develop a special legal institution of «digital ownership», which would reflect the possibility of exercising control, transferring or providing access to a token without violating the subject's right to its inherent identity. The second direction is the unification of concepts and procedures for identity tokenization within the international legal field. At the EU level, this unification can be achieved through the harmonization of eIDAS 2.0 with the W3C Verifiable Credentials 2.0 and DID technical specifications, as well as through the development of standard rules for the exchange of tokenized attributes between public and private systems. For EU partner countries, particularly Ukraine, it is crucial to establish a mechanism for the mutual recognition of tokenized identifiers in interstate electronic identification services, ensuring legal interoperability and cross-border trust.

The third step should be to integrate the principles of personal data protection into the tokenization process. It is necessary to ensure that all operations with a digital identity token fall under the principles of legality, proportionality and data minimization defined in the GDPR and national laws, while ensuring cryptographic verification without revealing sensitive information (through zero-knowledge proof and selective disclosure mechanisms). The next stage involves the formation of contractual and legal models for using the token, which will determine the scope of powers for the user, the service provider, and the verifying party. It is advisable to develop standard agreements and innovative contract templates that will enshrine the principle of «control without ownership» – the ability to manage digital attributes without fully transferring rights to them. Such a model will contribute to the introduction of a hybrid legal mechanism, in which ownership is understood as a dynamic system of entitlements, rather than as static possession. Thus, the improvement of legal regulation for tokenized forms of digital identity should be carried out based on a combination of three principles: technological neutrality, legal certainty, and personal sovereignty. Only such synergy will enable the reconciliation of the technological dynamics of the blockchain with classical concepts of property

rights, thereby creating the prerequisites for the formation of a new paradigm of digital citizenship in the global legal space.

Conclusions. As a result of the conducted research, it was found that the tokenization of digital identity is one of the key trends of digital transformation, which changes traditional ideas about ownership, control and personal rights in the virtual environment. The essence of tokenization is the transformation of intangible assets, particularly personal data and digital attributes of a person, into tokens capable of performing the functions of identification, verification, and access management. In the technological dimension, this process relies on blockchain architecture, smart contracts, decentralized identifiers and the concept of self-sovereign identity, which provide cryptographically verifiable user control over their own digital attributes.

An analysis of existing international approaches has shown that none of the considered legal systems recognizes a digital identity token as an object of full property rights. In the European Union, a regulatory model based on a combination of Regulation (EU) 2024/1183 (eIDAS 2.0) and GDPR dominates, where digital identity is interpreted as a set of personal attributes that are subject to the control of the data subject, but are not alienable. In the USA, on the other hand, a fragmented approach has been implemented: within the framework of UCC-2022 (Article 12), “control” over digital records is recognized as an analogue of possession; however, the lack of a single federal law on digital identity does not ensure the integrity of the legal regime. In Ukraine, legal regulation is developing towards harmonization with European standards through the Law «On Electronic Identification and Electronic Trust Services» and the implementation of the digital wallet «Diia». Singapore has adopted a centralized digital identity management model (NDI/Singpass), while integrating decentralized elements of Verifiable Credentials within the PDPA and IMDA/GovTech initiatives. In all jurisdictions, there is a common tendency to recognize identity tokens not as property, but as the authority to control and confirm an individual. It creates a need to develop a comprehensive regulatory framework

that combines the principles of property rights, personal data protection, and technological neutrality.

References

1. Boysen A. Decentralized, self-sovereign, consortium: The future of digital identity in Canada. *Frontiers in Blockchain.* 2021. Vol. 4. Article 624258. DOI: https://doi.org/10.3389/fbloc.2021.624258.

2. Garcia-Teruel R. M., Simón-Moreno H. The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*. 2021. Vol. 41. Article 105543. DOI: https://doi.org/10.1016/j.clsr.2021.105543.

3. Wang G., Nixon M. SoK: Tokenization on Blockchain. *2021 IEEE/ACM 14th International Conference on Utility and Cloud Computing (UCC '21) Companion*. 2021. Article 11. DOI: https://doi.org/10.1145/3492323.3495577.

4. Joshi S., Choudhury A. Tokenization of real estate assets using blockchain. *International Journal of Intelligent Information Technologies*. 2022. Vol. 18, № 3. P. 373-384. DOI: https://doi.org/10.4018/IJIIT.309588.

5. Kaptosv L. Using Redis for caching optimization in high-traffic web applications. *International Journal of Advanced Multidisciplinary Research and Studies.* 2025. Vol. 5, № 4. P. 1714-1722. DOI: https://doi.org/10.62225/2583049X.2025.5.4.4839.

6. Al-Ababneh H. A., Fedorchuk Y., Tymchyshyn A., Pishchenko G., Hrytsai S. The use of big data in the detection of economic crimes in public procurements. *Journal of Theoretical and Applied Information Technology*. 2024. Vol. 102, № 24. P. 8860-8871. URL: https://www.jatit.org/volumes/Vol102No24/3Vol102No24.pdf (date access: 05.09.2025).

7. Lee L. Examining the legal status of digital assets as property: a comparative analysis of jurisdictional approaches. *SSRN Electronic Journal*. 2024. DOI: http://dx.doi.org/10.2139/ssrn.4807135.

8. Sharif A., Ranzi M., Carbone R., Sciarretta G., Marino F. A., Ranise S. The eIDAS regulation: a survey of technological trends for European electronic identity schemes. *Applied Sciences*. 2022. Vol. 12, № 24. Article 12679. DOI: https://doi.org/10.3390/app122412679.

9. Kreppmeier J., Laschinger R., Steininger B. I., Dorfleitner G. Real estate security token offerings and the secondary market: driven by crypto hype or fundamentals? *Journal of Banking & Finance*. 2023. Vol. 154. Article 106940. DOI: https://doi.org/10.1016/j.jbankfin.2023.106940.

10. Ebadi R. Real estate tokenization: from theory to practice. *SSRN*. 2025. DOI: http://dx.doi.org/10.2139/ssrn.5366013.

11. Self-sovereign identity (SSI): autonomous identity management. 2024. URL: https://www.okta.com/identity-101/self-sovereign-identity (date access: 05.09.2025).

12. The past, present, and future of digital identity. 2024. URL: https://www.truvity.com/ssi-essentials/what-are-decentralized-identifiers (date access: 05.09.2025).

13. General data protection regulation 2016/679. URL: https://gdpr-info.eu/ (date access: 05.09.2025).

14. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng (date access: 05.09.2025).

15. Regulation (EU) 2024/1183 of 11 april 2024 amending regulation (EU) No 910/2014 (eIDAS 2.0). Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183 (date access: 05.09.2025).

16. Verifiable credentials data model v2.0 (15 May 2025). URL: https://www.w3.org/TR/vc-data-model-2.0/ (date access: 05.09.2025).

17. NIST. SP 800-63-4 digital identity guidelines (final, july 2025). URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf (date access: 05.09.2025).

18. California Privacy Protection Agency (CPPA). California Consumer Privacy Act / California Privacy Rights Act Regulations (2023–2024). URL: https://cppa.ca.gov/regulations/ (date access: 05.09.2025).

19. Singapore Personal Data Protection Commission (PDPC). Personal Data Protection Act (PDPA) Overview. URL: https://www.pdpc.gov.sg/who-we-are/about-us (date access: 05.09.2025).

20. Digital Utilities and Verifiable Credentials (TrustVC / SingVC) Framework. Infocomm Media Development Authority (IMDA).URL: https://www.imda.gov.sg/digital-economy/digital-utilities (date access: 05.09.2025).

21. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (date access: 05.11.2025).

22. Personal Data Protection Act. 2012. URL: https://sso.agc.gov.sg/Act/PDPA2012 (date access: 05.09.2025).

 ISSN: 3041-2110