Секція Право	
УДК 347.65:004.056:004.738.5	
Дата першого надходження статті до видання	2026-01-11
Дата прийняття статті до друку після рецензування	2026-02-25
Дата публікації/оприлюднення	2026-02-28

САМОСУВЕРЕННІ СИСТЕМИ ЦИФРОВОЇ СПАДЩИНИ: РОЗШИРЕННЯ РАМКИ ТУГОЛУКОВА–ЛЮШЕНКА ДЛЯ СПАДКУВАННЯ ЦИФРОВИХ АКТИВІВ В ЕКОСИСТЕМАХ WEB3

Перегуда Юлія А.
доктор економічних наук, доцент,
кафедра глобальної економіки,
Національний університет біоресурсів і природокористування України, Київ, Україна
e-mail: julilla.pereguda@gmail.com
https://orcid.org/0000-0002-1434-2509

Анотація. У статті досліджено проблему спадкування цифрових активів у Web3-екосистемах, де економічна цінність криптовалют, NFT, токенізованих активів, хмарно збережених об'єктів інтелектуальної власності та високовартісних платформних акаунтів не супроводжується достатньо надійними правовими й технічними механізмами міжгенераційної передачі. Актуальність теми зумовлена тим, що традиційне спадкове право орієнтоване переважно на матеріальні об'єкти або документально підтверджені майнові права, тоді як блокчейн-активи залежать від приватних ключів, платформні акаунти обмежуються умовами користування, а транскордонний характер цифрових портфелів ускладнює визначення застосовного права. Метою дослідження є розроблення інтегрованої концептуальної моделі Self-Sovereign Digital Heritage System (SSDHS), яка поєднує самосуверенну ідентичність, децентралізовані ідентифікатори, верифіковані облікові дані, цифрові сейфи, смарт-контрактне виконання спадкових умов і регуляторний комплаєнс. Методологічну основу становлять порівняльно-правовий аналіз, системний аналіз, функціональне моделювання, концептуальне проєктування та оцінювання регуляторного впливу. У роботі обґрунтовано шестирівневу архітектуру SSDHS, що охоплює рівень ідентичності, рівень інвентаризації цифрових активів, рівень захищеного зберігання, блокчейн-рівень, рівень спадкового виконання та рівень правової відповідності. Показано, що SSI вирішує проблему криптографічної автентифікації спадкоємця, тоді як цифровий сейф забезпечує безпечне зберігання приватних ключів, спадкових інструкцій, DID-матеріалу та цифрового заповіту. Проведено порівняльний аналіз регуляторних рамок США, Європейського Союзу й України щодо фідуціарного доступу до цифрових активів, електронних заповітів, цифрової ідентичності, ринку криптоактивів, захисту персональних даних, віртуальних активів та електронної ідентифікації. Доведено, що SSDHS може використовуватися як нормативно-технологічна референтна модель для зменшення ризику втрати цифрових активів через недоступність приватних ключів, підвищення надійності ідентифікації спадкоємців, скорочення залежності від централізованих посередників і підготовки майбутніх законодавчих рішень щодо цифрової спадщини.

Ключові слова: цифрове спадкування, цифрові активи, блокчейн, самосуверенна ідентичність, децентралізовані ідентифікатори, верифіковані облікові дані, цифровий сейф, Web3, смарт-контракти, цифрове спадкове планування, правові технології

e-ISSN: 2786-586X

SELF-SOVEREIGN DIGITAL HERITAGE SYSTEMS: EXTENDING THE TUHOLUKOV–LYUSHENKO FRAMEWORK FOR DIGITAL ASSET INHERITANCE IN WEB3 ECOSYSTEMS

Yuliia A. Pereguda
Doctor of Economics, Associate Professor,
Department of Global Economics,
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
e-mail: julilla.pereguda@gmail.com
https://orcid.org/0000-0002-1434-2509

Abstract. The article examines digital asset inheritance in Web3 ecosystems, where the economic value of cryptocurrencies, NFTs, tokenised assets, cloud-stored intellectual property and high-value platform accounts is not supported by sufficiently reliable legal and technical mechanisms for intergenerational transfer. The relevance of the topic is determined by the fact that traditional inheritance law is oriented mainly toward tangible objects or documented property rights, whereas blockchain-native assets depend on private keys, platform accounts are restricted by terms of service, and the cross-border nature of digital portfolios complicates the determination of applicable law. The purpose of the study is to develop an integrated conceptual model of the Self-Sovereign Digital Heritage System (SSDHS), combining self-sovereign identity, decentralised identifiers, verifiable credentials, digital safes, smart-contract execution of inheritance conditions and regulatory compliance. The methodological basis includes comparative legal analysis, system analysis, functional modelling, conceptual design and regulatory impact assessment. The article substantiates a six-layer SSDHS architecture consisting of the identity layer, digital asset inventory layer, secure storage layer, blockchain layer, inheritance execution layer and legal compliance layer. It is shown that SSI addresses the problem of cryptographic heir authentication, whereas the digital safe ensures secure preservation of private keys, inheritance instructions, DID material and the digital testament. A comparative analysis of the regulatory frameworks of the United States, the European Union and Ukraine is conducted, including fiduciary access to digital assets, electronic wills, digital identity, crypto-asset markets, personal data protection, virtual assets and electronic identification. The study substantiates that SSDHS can serve as a legal-technological reference model for reducing the risk of digital asset loss caused by inaccessible private keys, improving heir identification reliability, reducing dependence on centralised intermediaries and preparing future legislative solutions for digital heritage.

Keywords: digital inheritance, digital assets, blockchain, self-sovereign identity, decentralised identifiers, verifiable credentials, digital safe, Web3, smart contracts, digital estate planning, legal technology

Introduction

Relevance of the problem. The scale of digital asset accumulation over the past decade has created a distinct challenge for inheritance law and estate planning practice. Global cryptocurrency market capitalisation surpassed USD 2.5 trillion in early 2024, and the aggregate value of non-fungible tokens, tokenised real-world assets, decentralised finance positions, domain portfolios and high-value platform accounts adds to that figure. These assets are held not only by institutional investors but also by retail cryptocurrency users, digital creators, participants in decentralised autonomous organisations and owners of cloud-based services whose economic value is real while their transmissibility after death remains legally and technically uncertain.

The core technical problem is the dependence of blockchain-native assets on private cryptographic keys. Unlike a bank account or a documentary security, a blockchain asset is controlled through a key rather than through an institutional record. Loss of the key due to the death of the holder, hardware failure or physical destruction produces irreversible loss of access. Chainalysis estimates have repeatedly shown that a substantial share of Bitcoin supply may be

e-ISSN: 2786-586X

permanently inaccessible, with deceased holders and undocumented credentials forming one of the relevant causes of loss [1]. NFT collections, governance-token positions and DeFi protocol stakes usually do not contain a built-in succession mechanism.

The legal response remains fragmented. The Revised Uniform Fiduciary Access to Digital Assets Act in the United States creates a basis for fiduciary access to platform-based digital assets, but it does not solve the problem of self-custodied cryptographic assets [2]. The European Union has strengthened digital identity infrastructure through eIDAS 2.0 and regulated crypto-asset markets through MiCA, while a coordinated legal framework for digital asset inheritance has not yet emerged [3; 4]. Ukraine has adopted the Law on Virtual Assets, but the legal regime of inheritance of such assets remains incomplete [5].

The problem is not only legislative. Even where fiduciary access is allowed, the technical architecture of decentralised systems creates barriers that ordinary statutory amendments do not remove. A will cannot instruct a blockchain to release assets, a probate order cannot recover a lost private key, and a notarised authorisation is not automatically meaningful for a smart contract that executes on the basis of on-chain conditions. A workable solution must therefore combine legal recognition with technical enforceability.

Analysis of recent research and publications. The proposed approach is grounded in two research streams that are usually treated separately: self-sovereign identity as a trust architecture for Web3 environments and digital safes as infrastructure for the preservation and conditional transfer of digital estates. Tuholukov and Lyushenko analyse SSI as a basis for digital asset management in Web3, while Lyushenko, Sharafan and Tuholukov describe an information-technological architecture of digital safes for hereditary assets [6; 7]. These sources provide a useful starting point, but the model developed below is also based on a wider body of research on digital heritage, inheritance law, SSI standards, digital wallets and private international law.

The concept of digital heritage entered institutional and scholarly discourse through the UNESCO Charter on the Preservation of Digital Heritage, which defined digital heritage as special digital resources of human knowledge and expression and emphasised their fragility compared with conventional archival objects [8]. Harbinja demonstrated that many platforms treat user data not as property but as the object of a licence that may terminate upon death, thereby preventing ordinary succession of digital content [9]. Mazzone identified a related problem in social-media terms of service, where platforms effectively shape default post-mortem control over user content [10]. Beyer systematised the categories of digital property relevant to estate planning, while Carroll and Romano and Kasket developed the practical and social dimensions of digital afterlife [11; 12; 13].

A separate group of works deals with blockchain-native assets and smart contracts. Narayanan and co-authors formulated the irreversibility of private-key loss for cryptocurrency systems [14]. De Filippi and Wright extended this analysis to autonomous code execution, showing that smart contracts can produce legally significant effects that courts or probate authorities cannot easily reverse after execution [15]. Antonopoulos described multisignature and time-locked wallet mechanisms, which are technically relevant but insufficient as a comprehensive inheritance solution because they do not by themselves verify heirs or legal succession conditions [16]. Harbinja later underlined the gap between digital estates and the traditional legal treatment of assets on death [17].

The SSI paradigm emerged as a response to the limitations of centralised and federated identity models. Allen formulated the basic principles of SSI, including control, access, transparency, persistence, portability, interoperability, consent, minimisation and protection [18]. Mühle and co-authors identified the essential components of SSI ecosystems and showed that their viability depends on the interaction of DID methods, cryptographic primitives, wallets and trust policies [19]. The W3C DID v1.0 Recommendation defines decentralised identifiers as globally unique, cryptographically verifiable identifiers under the control of the subject [20]. The

e-ISSN: 2786-586X

W3C Verifiable Credentials Data Model v2.0 provides the corresponding attribute layer for signed claims that can be selectively disclosed by the holder [21].

Schardong and Custódio showed that SSI already has a developed taxonomy, although implementation maturity remains uneven [22]. Grüner, Mühle and Lockenvitz demonstrated that the main risks of SSI systems are often located not in the cryptographic core but in wallets, key recovery procedures and social engineering vectors [23]. Sedlmeir and co-authors described DIDs and Verifiable Credentials as a reproducible trust mechanism for inter-organisational processes [24]. Custers and Ursic, in policy commentary rather than a peer-reviewed legal article, discuss how SSI may be aligned with GDPR requirements through minimisation, selective disclosure and appropriate consent architecture [25].

Sources published in 2025 are particularly relevant to the updated evidentiary base of this study. Babel and co-authors clarify the relationship between SSI and digital wallets, emphasising governance, interoperability and the practical roles of issuers, holders and relying parties [26]. The European Digital Identity Wallet Architecture and Reference Framework specifies technical and organisational conditions for credential exchange within the EUDI Wallet ecosystem [27]. Further legal and socio-technical studies frame SSI as a digital identity infrastructure rather than merely a login tool [28; 29]. Blockchain-based KYC and credential models show how SSI can be integrated into regulated processes, but they also reveal the dependence of such systems on institutional trust anchors [30; 31; 32].

Recent studies of identity and access management, public digital identity infrastructure and concrete SSI implementations specify the conditions for large-scale deployment. Glöckler and co-authors systematise enterprise IAM requirements and the possible contribution of SSI [33]. Degen and Teubner analyse digital identity ecosystems from a government perspective [34]. Papatheodorou and co-authors present a secure blockchain-based SSI system that illustrates the practical feasibility of decentralised identity architectures [35]. Together, these works confirm that inheritance-oriented SSI cannot be designed as an isolated technical module; it requires institutional issuers, wallet governance, revocation mechanisms, secure key management and legally recognisable verification procedures.

Identification of the unresolved part of the problem. Despite the development of SSI and digital-safe research, these strands are rarely integrated into a single architecture for the inheritance of digital assets. The issuer-holder-verifier model has not been sufficiently mapped onto the role structure of succession, including civil registries, probate courts, notaries, executors and heirs. Digital safes have usually been discussed as secure storage environments, while SSI has been discussed as an identity layer. The unresolved problem is how to combine these elements into one legal-technological system capable of supporting digital inheritance in Web3 ecosystems.

Purpose of the article. The purpose of the article is to develop and justify an integrated Self-Sovereign Digital Heritage System (SSDHS) model for digital asset inheritance in Web3 ecosystems by combining SSI-based heir authentication, digital safe infrastructure, smart-contract execution and regulatory compliance mechanisms.

Scientific novelty. The scientific novelty lies in the proposed six-layer SSDHS architecture, the formal mapping of the issuer-holder-verifier SSI model onto inheritance roles, and the identification of posthumous DID custody as a separate architectural requirement for digital estate systems.

Practical significance. The practical significance of the study is that the SSDHS model can serve as a reference framework for digital estate planning, technical prototyping of digital safes, institutional credential issuance and legislative reform in the field of digital asset inheritance.

Methodology

Research methods. The study uses an interdisciplinary methodology that combines comparative legal analysis, system analysis, functional modelling, conceptual design and regulatory impact assessment. Comparative legal analysis is applied to the United States, the

e-ISSN: 2786-586X

European Union and Ukraine in order to identify convergent principles and structural gaps in the treatment of digital asset inheritance. The method is appropriate for a field in which national approaches are developing unevenly and where cross-border assets create practical obstacles to the legal effect of succession decisions.

System analysis decomposes digital inheritance into functional requirements: decentralised identification, secure long-term storage, conditional transfer of assets, cryptographic heir verification and regulatory compliance. The capacity of SSI and digital safe technologies to satisfy these requirements is assessed on the basis of technical standards, legal sources and published scholarship. The analysis is architectural rather than empirical: it specifies the components and relations that a system must contain before operational testing can be conducted.

Data sources. The source base consists of W3C DID and VC standards, EU materials on eIDAS 2.0, MiCA, the EUDI Wallet and succession regulation, Ukrainian legislation on inheritance, virtual assets, electronic identification and personal data protection, US uniform legislation on fiduciary access and electronic wills, and academic literature on digital inheritance, SSI, digital wallets, smart contracts and digital safes [1-50].

Analytical tools. The main analytical tools are functional decomposition, a comparative matrix of regulatory gaps, modelling of the succession event sequence and architectural mapping of SSI roles to succession roles. Functional decomposition is used to distinguish the identity layer, asset inventory layer, storage layer, blockchain layer, inheritance execution layer and compliance layer. The succession event sequence is described as a logical protocol rather than as a software diagram; therefore the article does not rely on UML, TOGAF, Zachman or another formal enterprise-architecture notation.

Regulatory impact assessment is used to determine the obstacles faced by SSDHS in the United States, the European Union and Ukraine. This approach separates the technical requirements of the system from the legal conditions without which its outputs would remain only technologically valid, but not legally effective. The method also allows the identification of specific amendments and institutional prerequisites needed for practical deployment.

Research limitations. The study is conceptual and architectural, not empirical. Its expected advantages are therefore described qualitatively: as potential reduction of private-key loss risk, improvement of heir authentication and reduction of dependence on centralised custodial intermediaries. The article does not present measured operational percentages, because such values would require pilot implementation, a comparative sample and longitudinal validation.

Results

The most significant legal obstacle to digital inheritance is definitional uncertainty. Most inheritance regimes were historically built around things, claims or documented property rights. Digital assets do not always fit neatly into these categories. A private key may control an economic value without itself being the asset; a token may represent a right, a claim, a licence, a governance position or merely a record in a protocol. Under Ukrainian law, the Law on Virtual Assets provides a statutory concept of virtual assets, but the operative inheritance regime remains incomplete [5]. At the same time, the Civil Code of Ukraine defines the estate primarily through rights and obligations that belonged to the deceased and did not cease upon death, while certain personal rights do not enter the estate; this makes the status of private keys, tokenised rights and platform accounts dependent on more precise legal qualification under succession law [36].

The cross-border nature of digital assets complicates the use of traditional conflict-of-laws rules. One holder may keep cryptocurrency through a foreign exchange, NFTs through a protocol associated with another jurisdiction, tokenised rights in a third country and cloud content under platform terms governed by another law. EU Succession Regulation No. 650/2012 creates a general framework for jurisdiction, applicable law and the European Certificate of Succession, but it does not specifically resolve the localisation or legal classification of blockchain-native assets

e-ISSN: 2786-586X

[47]. This creates uncertainty as to whether such assets should be treated as movables, claims, sui generis digital property or contractual positions.

Platform terms of service form a separate layer of restrictions. Many services do not provide for inheritance of an account, prohibit transfer of access, or allow only memorialisation or deletion. These contractual provisions may operate under the platform's governing law while frustrating rights that an heir would otherwise claim under the personal law of the deceased. RUFADAA addresses fiduciary access to platform-held digital assets in the United States, but it does not cover self-custodied cryptographic assets where no platform operator exists [2]. Electronic will legislation, including the Uniform Electronic Wills Act, may support the form of a digital testament but does not by itself create a technical mechanism for asset transfer [37].

From a technical perspective, the main barrier is dependence on the private key. In a self-custody environment, the private key functions as control over the asset: whoever has the key has access, and the loss of the key usually means a complete loss of access. This problem is not equivalent to an ordinary forgotten password, because there is often no central administrator capable of resetting credentials. It is therefore not enough for the testator to express an intention in a conventional will; the system must preserve the key material, verify the heir and release access only after legally relevant conditions are satisfied.

Heir authentication is the second technical problem. Even if the testator leaves a description of assets and instructions, the system must confirm death, heir status, compliance with testamentary conditions and the absence of contradictory legal restrictions. Smart contracts can execute on-chain logic, but they cannot independently know that an off-chain legal event has occurred. The relevant facts must be introduced through trusted credentials or oracles. This makes institutional issuers such as civil registries, courts and notaries essential to any legally meaningful digital inheritance system.

A further problem is the absence of a standardised digital inventory of the estate. Asset holders often rely on informal lists, password managers or private messages, but such tools do not create a legally coherent, machine-readable and updateable estate record. An inheritance system requires a structured inventory that links assets, controlling credentials, access conditions, heirs and legal instructions. Without this layer, even valid legal authority may be practically useless because heirs may not know what assets exist or how they are controlled.

At the organisational level, the gap lies in the absence of professional standards for digital estate planning. Lawyers and notaries often lack sufficient technical knowledge of private keys, wallets and smart contracts, while technical advisers often cannot determine the legal effect of testamentary acts, family status, probate orders or data-protection requirements. This division produces fragmented advice. A realistic system must therefore define the roles of legal professionals, technical custodians, institutional credential issuers and heirs in one architecture.

Self-sovereign identity addresses the problem of heir verification. In the SSI model, an authorised issuer creates and cryptographically signs a verifiable credential concerning a person or status; the holder stores it in a digital wallet; and the verifier checks the credential without needing permanent involvement of the issuer. In an inheritance scenario, a civil registry may issue a death credential, a notary may issue a testamentary credential, a court may issue a probate credential, and an heir may present a family-status credential. The verifier may be a smart-contract inheritance module or a digital safe access controller.

During the testator's lifetime, the testator can create a DID, prepare a digital testament and link the digital asset inventory to succession conditions. After death, the competent authority issues a verifiable death credential, while the heir presents credentials confirming identity, relationship or appointment as executor. The inheritance module verifies the issuer's signature, checks the status and validity of the credential, and compares the disclosed attributes with the conditions specified in the digital testament. This allows the system to verify legal facts without making a private company the gatekeeper of inheritance.

e-ISSN: 2786-586X

A key advantage of SSI is selective disclosure. An heir may confirm being a child of the testator, having reached a certain age or having executor status without disclosing all personal data to the system. This is important for GDPR-compatible design, because the storage and verification processes should operate on the minimum data needed for the succession purpose [38; 39]. The original eIDAS framework and its eIDAS 2.0 amendment provide the broader European legal context for electronic identification and trust services, although SSI categories still require careful legal mapping to recognised trust and wallet infrastructures [3; 40].

The digital safe performs a different but complementary function. It does not replace identity; it preserves the digital inventory, private keys, instructions, DID material, digital testament and audit records in encrypted form. Its architecture must satisfy two requirements at the same time: confidentiality during the testator's lifetime and availability to authorised heirs after death. The works on will expression and digital asset inheritance in Ukrainian legal scholarship show that this problem cannot be reduced either to a purely contractual act or to a purely technical storage arrangement [41; 42].

Functionally, the digital safe should perform at least three operations. The first is long-term encrypted storage of assets, keys, instructions and documents. The second is management of access conditions, allowing staged release of different types of material. The third is integration with heir authentication, so that access is granted only after presentation of valid credentials. This architecture is stronger than a simple password manager or hardware wallet backup, because it connects access to verifiable legal conditions rather than to possession of a secret alone.

The integration of SSI and the digital safe removes the weaknesses of each approach separately. SSI can verify the legal status of the heir, but it does not itself store asset keys. The digital safe can preserve keys, but it cannot by itself determine whether the requesting party is legally entitled to access them. SSDHS combines both functions and adds an inheritance execution layer. The special requirement of posthumous DID custody follows from this integration: if the testator's DID is needed to activate or validate the succession process, the DID key material must be preserved and released under conditions comparable to the preservation of asset keys. Research on key rotation, blockchain identity management and accessible SSI interfaces confirms the importance of key-management and wallet-usability design for such systems [43; 44; 45].

The SSDHS model consists of six functional layers. The first is the identity layer, which includes DIDs, verifiable credentials and SSI wallets of the testator, heirs, notaries, courts and civil registries. The second is the asset inventory layer, which records cryptocurrencies, tokens, platform accounts, digital intellectual property and other digital assets together with the credentials or instructions needed to control them. The third is the storage layer, represented by the digital safe, where the inventory, private keys, DID material, digital testament and audit logs are stored in encrypted form.

The fourth layer is the blockchain registry, which supports DID resolution, signature verification, smart-contract execution and immutable audit records, but should not store personal data or detailed asset inventories. The fifth layer is the inheritance execution layer, which contains the logic of the digital testament and determines when and how assets or access credentials are released. The sixth layer is the compliance layer, which connects technical execution with the requirements of succession law, electronic identification law, data protection, crypto-asset regulation and professional obligations of notaries, courts or custodians.

The succession event sequence in SSDHS is a staged protocol. First, the death of the testator is registered by the competent authority, which issues a verifiable death credential linked to the testator's DID. Second, the inheritance smart contract or inheritance module verifies the credential and activates the succession protocol. Third, the system notifies designated heirs and, where applicable, the executor or trustee. Fourth, the heirs present their SSI credentials through a wallet. Fifth, the system verifies issuers, signatures, validity periods, revocation status and relevant attributes.

e-ISSN: 2786-586X

After successful verification, the inheritance module issues an authorisation to the digital safe. The authorisation specifies which components of the digital inventory the verified heir may access and under what conditions. For blockchain-native assets, this may involve release of controlling private keys or activation of a transfer transaction. For platform accounts or off-chain rights, the safe may disclose instructions, credentials or documentary evidence needed for interaction with a service provider or probate authority. Each action is recorded in an audit log that can be used in probate or regulatory review.

The comparative regulatory analysis shows that the United States has a relatively developed model of fiduciary access to platform-held digital assets through RUFADAA, while electronic will legislation supports the possibility of electronic testamentary forms [2; 37]. The unresolved issue is that self-custodied crypto-assets do not have an operator to whom a fiduciary demand can be addressed. Digital identity in the US is also based on assurance and federation standards rather than on a single SSI infrastructure. NIST SP 800-63-4 therefore provides a more current reference point for digital identity assurance than older policy documents, but it does not by itself give DID-based succession credentials procedural force in probate matters [50].

The European Union has more favourable conditions for SSDHS because eIDAS 2.0 and the EUDI Wallet create a path toward institutionally issued and wallet-presented attributes [3; 27]. The point is not that all citizens must use a wallet, but that Member States must make a European Digital Identity Wallet available and that recognised relying parties must accept relevant credentials in defined contexts. If civil registries, notaries or courts issue death, family-status or probate credentials in a legally recognised format, the identity layer of SSDHS could operate inside a recognised digital identity ecosystem. MiCA is relevant for custodians and crypto-asset service providers, but it does not contain a complete inheritance regime for digital assets [4]. EU Succession Regulation No. 650/2012 supplies a general succession framework, while an explicit digital-asset component remains absent [47].

Ukraine faces the largest implementation gap but also has a clear reform path. The current Law of Ukraine “On Electronic Identification and Electronic Trust Services” No. 2155-VIII regulates electronic identification and trust services, but it does not introduce SSI, DID or verifiable credentials as legal categories in the sense required for the SSDHS model [38]. The Law on Virtual Assets provides a starting point for the legal treatment of virtual assets, but succession mechanisms for such assets remain undeveloped [5]. The Civil Code of Ukraine would also need interpretive or legislative clarification on whether tokenised assets, access credentials and certain platform rights fall within the estate [36].

A Ukrainian reform pathway should include recognition of SSI, DID and VC concepts; determination of the legal force of verifiable credentials issued by civil registries, courts and notaries; activation and supplementation of virtual-asset legislation with inheritance-specific provisions; development of a digital estate planning standard; and pilot integration with national digital infrastructure. Such reforms would also need to comply with personal data protection requirements and with eventual convergence toward European digital identity rules [39; 40].

International coordination remains underdeveloped. The HCCH Digital Tokens Project directly addresses private international law issues raised by digital tokens, including problems of localisation and applicable law [48]. UNCITRAL’s Model Law on Electronic Transferable Records offers a useful example of functional equivalence for electronic records, although it does not create a regime for inheritance of crypto-assets as such [49]. These instruments are important reference points, but no binding international instrument currently resolves cross-border digital asset succession, mutual recognition of succession credentials or the legal status of posthumous access to self-custodied assets.

The comparison of the United States, the European Union and Ukraine confirms a common pattern: each jurisdiction contains some elements of a future system, but none has a complete legal and technical cycle for Web3 inheritance. The United States is stronger in fiduciary access to platform accounts, the European Union in digital identity infrastructure and succession conflict

e-ISSN: 2786-586X

rules, and Ukraine in the potential for convergence with EU approaches through legal reform. A complete SSDHS deployment would therefore require not only software development, but also legal recognition of credentials, professional standards and cross-border coordination.

Discussion

Interpretation of results. The SSDHS model shows that digital inheritance cannot be solved only through amendments to inheritance law or through a separate technical backup service. The problem is hybrid: legal facts must be verifiable in a technical environment, while technical execution must remain connected to legally valid succession conditions. SSI and digital safes therefore perform different but interdependent functions. SSI verifies the identity and status of the heir; the digital safe preserves assets, keys and instructions; the inheritance layer links verified facts with access or transfer.

At the technical level, SSDHS reduces the risk of complete asset loss because inventory management, encrypted storage and staged release of key material become part of the system design. At the legal level, the compliance layer prevents purely technical execution from replacing succession law. At the organisational level, the model distributes responsibilities among the testator, heirs, notaries, registries, courts, custodians and verifiers. This structure makes the model more realistic than solutions based only on multisignature wallets, password managers or platform memorialisation tools.

The expected effects of the model should be interpreted cautiously. On the basis of its architecture, one may expect a reduction in the risk of digital asset loss due to inaccessible private keys, less dependence on centralised intermediaries and more reliable heir identification. These results are not quantified in this article. They should be treated as hypotheses for pilot testing rather than as empirically proven indicators.

Posthumous DID custody requires special attention. If the testator's DID is needed to activate the digital testament, verify the relationship between assets and succession conditions, or confirm the origin of instructions, loss of DID key material may block the process in the same way as loss of a private key to a cryptocurrency wallet. The digital safe must therefore preserve not only asset keys but also identity-control material. This requirement distinguishes SSDHS from ordinary wallet recovery systems.

Comparison with other studies. The findings are consistent with SSI literature that treats decentralised identity as an institutional trust architecture with issuers, holders and verifiers rather than as a simple authentication technology [18; 19; 22; 24]. More recent research on digital wallets and IAM processes confirms that the viability of SSI depends on governance, credential interoperability, key security and the participation of institutional issuers [26; 33; 34]. The present model extends digital-safe research by connecting secure storage and succession instructions with DID-based heir authentication and posthumous DID key custody [7].

Scientific novelty in detail. The extended scientific novelty lies in describing SSDHS not as a general model of digital identity or data storage, but as a specialised inheritance architecture. It combines identity, asset inventory, secure storage, blockchain registry, inheritance execution and compliance layers. It also describes the transition from the legal fact of death to heir verification and asset transfer. The additional contribution is the separation of posthumous DID custody as an independent component of digital estate planning.

Practical significance in detail. The practical value of SSDHS lies in its possible use for the design of digital inheritance services, technical requirements for digital safes, notarial procedures involving digital assets, institutional credential issuance and future legislative reform. For asset holders, the model offers a structured way to record and transmit assets that would otherwise remain invisible to heirs. For legal professionals, it clarifies which technical components must be considered when advising on digital estates. For regulators, it provides a reference architecture that can be translated into legal definitions, procedural rules and certification requirements.

e-ISSN: 2786-586X

Conclusions

The study substantiates the Self-Sovereign Digital Heritage System as a six-layer architecture for digital asset inheritance in Web3 ecosystems. The proposed model combines self-sovereign identity, digital asset inventory, a secure digital safe, a blockchain registry, smart-contract inheritance execution and a compliance layer. This structure allows digital inheritance to be treated not as a purely legal or purely technical problem, but as a legal-technological process requiring coordination between institutions, credentials and cryptographic control mechanisms.

Self-sovereign identity is a necessary component of digital inheritance because it enables cryptographically verifiable heir authentication without constant dependence on a centralised intermediary. Inheritance requires confirmation of death, identity, kinship, appointment, age or other legal conditions. SSI allows these facts to be expressed through verifiable credentials issued by competent institutions and presented selectively by heirs.

The digital safe is the infrastructural core of digital heritage preservation. Its function is not limited to storing private keys. It must also support the estate inventory, inheritance instructions, digital testament, DID material and audit records. The integration of a digital safe with SSI allows the system to connect secure preservation with legally relevant access conditions.

The central architectural conclusion is that SSI and digital safes do not duplicate each other. They solve different parts of the same problem. SSI is responsible for trusted identification and verification of succession status; the digital safe is responsible for preserving key material and instructions; the inheritance execution layer connects these elements into an operational protocol. The requirement of posthumous DID custody is the most specific contribution of the model, because it treats identity-control material as a separate object of succession-sensitive preservation.

The comparative analysis of the United States, the European Union and Ukraine shows that no jurisdiction yet has a complete framework for Web3 inheritance. The United States has more developed tools for fiduciary access to platform assets. The European Union has stronger digital identity and cross-border succession infrastructure. Ukraine requires legal clarification of virtual assets, electronic identification and the inheritance status of tokenised and key-controlled assets. International coordination remains necessary because digital assets are not confined to one territory or legal system.

Further research should move from conceptual architecture to pilot verification. The most relevant pilot would involve a civil registry capable of issuing a verifiable death credential, a notarial or probate institution willing to recognise SSI-based heir authentication, and a digital-safe provider able to preserve both asset keys and DID key material. Such a pilot would allow testing of legal validity, technical reliability, user experience and cross-jurisdictional recognition under controlled conditions.

Список використаних джерел

1. Chainalysis. The Chainalysis 2020 Crypto Crime Report. Chainalysis Inc., 2020. URL: https://go.chainalysis.com/2020-Crypto-Crime-Report.html (дата звернення: 18.12.2025).
2. Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). Uniform Law Commission, 2015. URL: https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22 (дата звернення: 18.12.2025).
3. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj (дата звернення: 18.12.2025).
4. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets. Official Journal of the European Union. 2023. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj (дата звернення: 18.12.2025).
5. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20 (дата звернення: 18.12.2025).

e-ISSN: 2786-586X

6. Tuholukov O., Lyushenko D. Self-sovereign identity as the basis for digital asset management in the Web3 environment. Ukrainian Political and Legal Discourse. 2025. № 16. DOI: https://doi.org/10.5281/zenodo.17532852.
7. Люшенко Д., Шарафан Р., Туголуков О. Інформаційні технології у створенні «цифрових сейфів» для зберігання спадкових активів. Наука і техніка сьогодні. 2025. Вип. 9, № 50. С. 1304–1321. DOI: https://doi.org/10.52058/2786-6025-2025-9(50)-1304-1321.
8. UNESCO. Charter on the Preservation of Digital Heritage. UNESCO General Conference, 32nd Session. Paris, 2003. URL: https://unesdoc.unesco.org/ark:/48223/pf0000179529.page=2 (дата звернення: 18.12.2025).
9. Harbinja E. Legal aspects of transmission of digital assets on death : doctoral dissertation. University of Strathclyde, 2017.
10. Mazzone J. Facebook's afterlife. North Carolina Law Review. 2012. Vol. 90, № 5. P. 1643–1694.
11. Beyer G. W. Estate planning in the digital age: managing digital assets. Trusts & Estates. 2016. Vol. 155, № 6. P. 12–18.
12. Carroll J., Romano A. Your Digital Afterlife: When Facebook, Flickr and Twitter Are Your Estate, What's Your Digital Executor to Do? New Riders, 2011.
13. Kasket E. All the Digital Strangers: How Technology Shapes Our Afterlife. Little, Brown Book Group, 2019.
14. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies. Princeton : Princeton University Press, 2016.
15. De Filippi P., Wright A. Blockchain and the Law: The Rule of Code. Harvard University Press, 2018.
16. Antonopoulos A. M. Mastering Bitcoin: Programming the Open Blockchain. 2nd ed. O'Reilly Media, 2017.
17. Harbinja E. Digital estates and avatars: a brief overview of the legal treatment of digital assets on death. Journal of Media Law. 2019. Vol. 11, № 1. P. 1–25.
18. Allen C. The path to self-sovereign identity. Life With Alacrity. 2016. URL: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity (дата звернення: 18.12.2025).
19. 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.
20. W3C. Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. W3C Recommendation. 2022. URL: https://www.w3.org/TR/did-1.0/ (дата звернення: 18.12.2025).
21. W3C. Verifiable Credentials Data Model v2.0. W3C Recommendation. 2025. URL: https://www.w3.org/TR/vc-data-model-2.0/ (дата звернення: 18.12.2025).
22. Schardong F., Custódio R. Self-sovereign identity: a systematic review, mapping and taxonomy. Sensors. 2022. Vol. 22, № 15. Article 5641. DOI: https://doi.org/10.3390/s22155641.
23. 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.
24. Sedlmeir J., Smethurst R., Rieger A., Fridgen G. Digital identities and verifiable credentials. Business & Information Systems Engineering. 2021. Vol. 63, № 5. P. 603–613. DOI: https://doi.org/10.1007/s12599-021-00722-y.
25. 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/ (дата звернення: 18.12.2025).
26. Babel M., Willburger L., Lautenschlager J. et al. Self-sovereign identity and digital wallets. Electronic Markets. 2025. Vol. 35. Article 28. DOI: https://doi.org/10.1007/s12525-025-00772-0.

e-ISSN: 2786-586X

27. European Commission. European Digital Identity Wallet Architecture and Reference Framework. Version 1.10.0. 2025. URL: https://eudi.dev/1.10.0/architecture-and-reference-framework-main/ (дата звернення: 18.12.2025).
28. Giannopoulou A., Wang F. Self-sovereign identity. Internet Policy Review. 2021. Vol. 10, № 2. DOI: https://doi.org/10.14763/2021.2.1550.
29. Giannopoulou A. Digital identity infrastructures: a critical approach of self-sovereign identity. Digital Society. 2023. Vol. 2. Article 18. DOI: https://doi.org/10.1007/s44206-023-00049-z.
30. Ferdous M. S., Chowdhury F., Alassafi M. O. In search of self-sovereign identity leveraging blockchain technology. IEEE Access. 2019. Vol. 7. P. 103059–103079. DOI: https://doi.org/10.1109/ACCESS.2019.2931173.
31. Wang F., De Filippi P. Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. Frontiers in Blockchain. 2020. Vol. 2. Article 28. DOI: https://doi.org/10.3389/fbloc.2019.00028.
32. Schlatt V., Sedlmeir J., Feulner S., Urbach N. Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management. 2021. Vol. 59, № 7. Article 103553. DOI: https://doi.org/10.1016/j.im.2021.103553.
33. Glöckler J., Sedlmeir J., Frank M., Fridgen G. A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Business & Information Systems Engineering. 2024. Vol. 66. P. 421–440. DOI: https://doi.org/10.1007/s12599-023-00830-x.
34. Degen K., Teubner T. Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. Electronic Markets. 2024. Vol. 34. Article 50. DOI: https://doi.org/10.1007/s12525-024-00731-1.
35. Papatheodorou N., Karras A., Theodorakopoulos L., Karras C. The YouGovern secure blockchain-based self-sovereign identity system. Applied Sciences. 2025. Vol. 15, № 12. Article 6437. DOI: https://doi.org/10.3390/app15126437.
36. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/go/435-15 (дата звернення: 18.12.2025).
37. Uniform Law Commission. Uniform Electronic Wills Act. 2019. URL: https://www.uniformlaws.org/committees/community-home?CommunityKey=a0a16f19-97a8-4f86-afc1-b1c0e051fc71 (дата звернення: 18.12.2025).
38. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2155-19 (дата звернення: 18.12.2025).
39. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 18.12.2025).
40. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 18.12.2025).
41. 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. Official Journal of the European Union. 2014. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj (дата звернення: 18.12.2025).
42. 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.
43. Шаповал К. О., Наконечна Д. О. Спадкування цифрових активів: особливості регулювання. Юридичний науковий електронний журнал. 2025. № 4. С. 160–165. DOI: https://doi.org/10.32782/2524-0374/2025-4/36.

e-ISSN: 2786-586X

44. 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.
45. 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.
46. Lockwood M. An accessible interface layer for self-sovereign identity. Frontiers in Blockchain. 2021. Vol. 3. Article 609101. DOI: https://doi.org/10.3389/fbloc.2020.609101.
47. Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession. Official Journal of the European Union. 2012. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R0650 (дата звернення: 18.12.2025).
48. Hague Conference on Private International Law. Digital Tokens Project. URL: https://www.hcch.net/en/projects/legislative-projects/digital-tokens1 (дата звернення: 18.12.2025).
49. UNCITRAL. Model Law on Electronic Transferable Records. 2017. URL: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records (дата звернення: 18.12.2025).
50. National Institute of Standards and Technology. Digital Identity Guidelines: Special Publication 800-63-4. 2025. URL: https://pages.nist.gov/800-63-4/ (дата звернення: 18.12.2025).

References

1. Chainalysis. (2020). The Chainalysis 2020 Crypto Crime Report. Chainalysis Inc. https://go.chainalysis.com/2020-Crypto-Crime-Report.html
2. Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). (2015). Uniform Law Commission. https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22
3. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. (2024). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1183/oj
4. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets. (2023). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/1114/oj
5. Law of Ukraine On Virtual Assets No. 2074-IX. (2022, February 17). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2074-20
6. Tuholukov, O., & Lyushenko, D. (2025). Self-sovereign identity as the basis for digital asset management in the Web3 environment. Ukrainian Political and Legal Discourse, 16. https://doi.org/10.5281/zenodo.17532852
7. Lyushenko, D., Sharafan, R., & Tuholukov, O. (2025). Informatsiini tekhnolohii u stvorenni “tsyfrovykh seifiv” dlia zberihannia spadkovykh aktyviv [Information technologies in creating digital safes for the storage of hereditary assets]. Nauka i Tekhnika Sogodni, 9(50), 1304–1321. https://doi.org/10.52058/2786-6025-2025-9(50)-1304-1321
8. UNESCO. (2003). Charter on the Preservation of Digital Heritage. UNESCO General Conference, 32nd Session, Paris. https://unesdoc.unesco.org/ark:/48223/pf0000179529.page=2
9. Harbinja, E. (2017). Legal aspects of transmission of digital assets on death [Doctoral dissertation, University of Strathclyde].
10. Mazzone, J. (2012). Facebook’s afterlife. North Carolina Law Review, 90(5), 1643–1694.
11. Beyer, G. W. (2016). Estate planning in the digital age: Managing digital assets. Trusts & Estates, 155(6), 12–18.

e-ISSN: 2786-586X

12. Carroll, J., & Romano, A. (2011). Your Digital Afterlife: When Facebook, Flickr and Twitter Are Your Estate, What's Your Digital Executor to Do? New Riders.
13. Kasket, E. (2019). All the Digital Strangers: How Technology Shapes Our Afterlife. Little, Brown Book Group.
14. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies. Princeton University Press.
15. De Filippi, P., & Wright, A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.
16. Antonopoulos, A. M. (2017). Mastering Bitcoin: Programming the Open Blockchain (2nd ed.). O'Reilly Media.
17. Harbinja, E. (2019). Digital estates and avatars: A brief overview of the legal treatment of digital assets on death. Journal of Media Law, 11(1), 1–25.
18. Allen, C. (2016). The path to self-sovereign identity. Life With Alacrity. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity
19. Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
20. W3C. (2022). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations. W3C Recommendation. https://www.w3.org/TR/did-1.0/
21. W3C. (2025). Verifiable Credentials Data Model v2.0. W3C Recommendation. https://www.w3.org/TR/vc-data-model-2.0/
22. Schardong, F., & Custódio, R. (2022). Self-sovereign identity: A systematic review, mapping and taxonomy. Sensors, 22(15), 5641. https://doi.org/10.3390/s22155641
23. Grüner, A., Mühle, A., & Lockenvitz, N. (2023). Analyzing and comparing the security of self-sovereign identity management systems through threat modeling. International Journal of Information Security, 22, 1231–1248. https://doi.org/10.1007/s10207-023-00688-w
24. Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. Business & Information Systems Engineering, 63(5), 603–613. https://doi.org/10.1007/s12599-021-00722-y
25. Custers, B., & Ursic, H. (2023). Can self-sovereign identity (SSI) fit within the GDPR? CiTiP Blog, KU Leuven. https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-fit-within-the-gdpr-part-i/
26. Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M.-F., Sedlmeir, J., Strüker, J., & Urbach, N. (2025). Self-sovereign identity and digital wallets. Electronic Markets, 35, Article 28. https://doi.org/10.1007/s12525-025-00772-0
27. European Commission. (2025). European Digital Identity Wallet Architecture and Reference Framework, version 1.10.0. https://eudi.dev/1.10.0/architecture-and-reference-framework-main/
28. Giannopoulou, A., & Wang, F. (2021). Self-sovereign identity. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1550
29. Giannopoulou, A. (2023). Digital identity infrastructures: A critical approach of self-sovereign identity. Digital Society, 2, Article 18. https://doi.org/10.1007/s44206-023-00049-z
30. Ferdous, M. S., Chowdhury, F., & Alassafi, M. O. (2019). In search of self-sovereign identity leveraging blockchain technology. IEEE Access, 7, 103059–103079. https://doi.org/10.1109/ACCESS.2019.2931173
31. Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. Frontiers in Blockchain, 2, Article 28. https://doi.org/10.3389/fbloc.2019.00028
32. Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2021). Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management, 59(7), Article 103553. https://doi.org/10.1016/j.im.2021.103553

e-ISSN: 2786-586X

33. Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Business & Information Systems Engineering, 66, 421–440. https://doi.org/10.1007/s12599-023-00830-x
34. Degen, K., & Teubner, T. (2024). Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. Electronic Markets, 34, Article 50. https://doi.org/10.1007/s12525-024-00731-1
35. Papatheodorou, N., Karras, A., Theodorakopoulos, L., & Karras, C. (2025). The YouGovern secure blockchain-based self-sovereign identity system. Applied Sciences, 15(12), 6437. https://doi.org/10.3390/app15126437
36. Civil Code of Ukraine No. 435-IV. (2003, January 16). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/go/435-15
37. Uniform Law Commission. (2019). Uniform Electronic Wills Act. https://www.uniformlaws.org/committees/community-home?CommunityKey=a0a16f19-97a8-4f86-afc1-b1c0e051fc71
38. Law of Ukraine On Electronic Identification and Electronic Trust Services No. 2155-VIII. (2017, October 5). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/go/2155-19
39. Law of Ukraine On Personal Data Protection No. 2297-VI. (2010, June 1). Verkhovna Rada of Ukraine. https://zakon.rada.gov.ua/laws/show/2297-17
40. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). (2016). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
41. 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. (2014). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2014/910/oj
42. Savchenko, V., & Maydanyk, R. (2024). Contracts implied-in-fact like a form of will expression. Access to Justice in Eastern Europe, 7(2), 283–300. https://doi.org/10.33327/AJEE18-7.2-a000212
43. Shapoval, K. O., & Nakonechna, D. O. (2025). Spadkuvannia tsyfrovykh aktyviv: osoblyvosti rehuliuvannia [Inheritance of digital assets: regulatory features]. Yurydychnyi Naukovyi Elektronnyi Zhurnal, 4, 160–165. https://doi.org/10.32782/2524-0374/2025-4/36
44. Park, C. S., & Nam, H. M. (2021). A new approach to constructing decentralized identifier for secure and flexible key rotation. IEEE Internet of Things Journal, 9(13), 10610–10624. https://doi.org/10.1109/JIOT.2021.3121722
45. Kuperberg, M. (2020). Blockchain-based identity management: A survey from the enterprise and ecosystem perspective. IEEE Transactions on Engineering Management, 67(4), 1008–1027. https://doi.org/10.1109/TEM.2019.2926471
46. Lockwood, M. (2021). An accessible interface layer for self-sovereign identity. Frontiers in Blockchain, 3, 609101. https://doi.org/10.3389/fbloc.2020.609101
47. Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession. (2012). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R0650
48. Hague Conference on Private International Law. (n.d.). Digital Tokens Project. https://www.hcch.net/en/projects/legislative-projects/digital-tokens1
49. UNCITRAL. (2017). Model Law on Electronic Transferable Records. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
50. National Institute of Standards and Technology. (2025). Digital Identity Guidelines: Special Publication 800-63-4. https://pages.nist.gov/800-63-4/

e-ISSN: 2786-586X