МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
КАФЕДРА ІНТЕЛЕКУАЛЬНОЇ ВЛАСНОСТІ ТА ІНФОРМАЦІЙНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

Смірнова Ігоря Сергійовича

УДК 34:004.9(043.3)

Д И С Е Р Т А Ц І Я

"Правове регулювання інформаційних відносин, що виникають у зв'язку із застосуванням блокчейн – технології"

081 "Право"

Право

Подається на здобуття наукового ступеня доктора філософії за спеціальністю 081 "Право".

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ І.С. Смірнов.

Науковий керівник (консультант) Кодинець Анатолій Олександрович – доктор юридичних наук, професор кафедри інтелектуальної власності та інформаційного права.

Київ – 2026 рік

А Н О Т А Ц І Я

Смірнов І.С. Правове регулювання інформаційних відносин, що виникають у зв’язку із застосуванням блокчейн-технології. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 "Право". – Київський національний університет імені Тараса Шевченка, Київ, 2026 рік.

У дисертації представлено комплексне дослідження правових засад регулювання інформаційних відносин, що виникають при застосуванні блокчейн-технології в сучасному цифровому середовищі. Необхідність удосконалення законодавчого регулювання зумовлена стрімким поширенням децентралізованих мереж, їхнім багатовимірним впливом на економічну, правову та соціальну сфери, а також формуванням нових правових механізмів управління віртуальними активами, включаючи криптовалюти, токени та смарт-контракти.

У першому розділі проаналізовано теоретико-правові основи блокчейн-технології як унікального феномену сучасного інформаційного суспільства. З урахуванням етапів розвитку розподілених реєстрів досліджено базові принципи блокчейну (децентралізація, незмінність записів, криптографічний захист) та їх безпосередній вплив на правовідносини, що формуються в цьому технологічному середовищі. Доведено, що розуміння сутності блокчейну та пов'язаних із ним інформаційних процесів дозволяє визначити особливості правового статусу учасників (користувачів, майнерів, розробників, регуляторів), їхні взаємні права й обов'язки, та з'ясувати роль інформаційного компонента в цифрових правочинах.

Другий розділ присвячено цивільно-правовим аспектам використання блокчейн-технологій, зокрема розкрито правову природу віртуальних активів (криптовалют, токенів, NFT). Запропоновано класифікацію віртуальних активів за функціональним призначенням, економічною сутністю, ліквідністю та можливістю використання як засобу платежу. Особливу увагу зосереджено на смарт-контрактах: обґрунтовано їх розуміння як електронної форми правочину, де умови зафіксовано у програмному

коді, а виконання відбувається автоматизовано. Виявлено, що відсутність спеціального законодавчого регулювання смарт-контрактів створює правові ризики, пов'язані з визначенням волевиявлення сторін, механізмами внесення змін та вирішенням спорів. Доведено, що смарт-контракти можуть стати ефективним інструментом забезпечення виконання зобов'язань у різних сферах – від фінансових операцій до управління правами інтелектуальної власності.

Третій розділ зосереджено на міжнародно-правовому досвіді та механізмах захисту прав учасників блокчейн-відносин. Здійснено порівняльний аналіз моделей регулювання криптовалют і децентралізованих фінансів у різних юрисдикціях: Європейському Союзі (директиви, регламент MiCA), США (підходи SEC, CFTC), Китаї (обмеження криптодіяльності при розвитку державного цифрового юаня), а також у Швейцарії, Сінгапурі та Японії. Встановлено, що відсутність гармонізованих міжнародних стандартів у сфері блокчейну спричиняє колізії правових норм, ускладнює транскордонні операції та потребує активнішої ролі міжнародних організацій (FATF, ISO, WIPO). Досліджено питання захисту інтелектуальної власності у Web3, регулювання NFT та цифрових контент-платформ, а також проблематику забезпечення конфіденційності даних, включаючи конфлікт із вимогами GDPR щодо "права на забуття".

Четвертий розділ присвячено перспективам удосконалення правового регулювання блокчейн-технологій в Україні. Проаналізовано сучасний стан нормативно-правової бази, включаючи Закон України "Про віртуальні активи", підзаконні акти та роль регуляторних органів. Сформульовано рекомендації щодо впровадження "регуляторних пісочниць" для блокчейн-проєктів, що дозволить тестувати інноваційні рішення з мінімальними ризиками. Обґрунтовано доцільність розвитку концепції smart government через впровадження блокчейну в державні реєстри, публічні закупівлі та електронне голосування. Доведено, що інтеграція децентралізованих технологій у державний сектор сприятиме підвищенню прозорості, зменшенню корупційних ризиків та оптимізації адміністративних процедур.

Наукова новизна полягає в комплексному, міждисциплінарному аналізі блокчейну як правового феномену, що поєднує елементи інформаційного, цивільного, фінансового та міжнародного права. Систематизовано концепції трансформації управління інформаційними ресурсами через децентралізацію та запропоновано підходи до правової кваліфікації віртуальних активів. Уперше в українській правовій доктрині блокчейн досліджено не лише як інструмент криптовалютних операцій, але і як механізм захисту прав інтелектуальної власності, забезпечення прозорості бізнес-процесів та модернізації державного управління.

Практичне значення результатів полягає в можливості їх застосування при розробці нормативно-правових актів, підготовці законопроєктів щодо віртуальних активів і смарт-контрактів, удосконаленні Цивільного кодексу України. Крім того, запропоновані концепції можуть використовуватися при формуванні спеціалізованих навчальних дисциплін та програм підвищення кваліфікації фахівців у галузі цифрового права, IT-права та інтелектуальної власності.

Зроблено висновок, що впровадження блокчейн-технологій в Україні може стати каталізатором цифрової трансформації, забезпечивши формування прозорих та передбачуваних правил функціонування ринку. Водночас повноцінна реалізація потенціалу блокчейну потребує вдосконалення законодавчих механізмів захисту прав учасників, регулювання діяльності майнерів та операторів віртуальних активів, впровадження ефективних інструментів протидії шахрайству та легалізації незаконних доходів. Важливим є врахування міжнародного досвіду, зокрема регуляторних підходів ЄС, рекомендацій FATF та практик провідних країн, для забезпечення сумісності правових систем та залучення іноземних інвестицій у вітчизняну блокчейн-інфраструктуру.

Таким чином, дисертаційне дослідження розкриває правову природу та механізми функціонування інформаційних відносин у розподілених мережах, визначає місце й роль блокчейн-технології в системі сучасного права та пропонує комплекс законодавчих і практичних рекомендацій для формування ефективної нормативної бази. Отримані результати створюють фундамент для подальших

наукових досліджень у сфері цифрових технологій, інтелектуальної власності, електронної комерції та правового забезпечення інновацій.

Ключові слова: *блокчейн-технологія, інформаційні відносини, правове регулювання, віртуальні активи, криптовалюта, смарт-контракти, NFT, захист прав інтелектуальної власності, авторське право, інформаційно-комунікаційні технології, цифрове середовище, адаптація законодавства до ЄС*.

Список публікацій здобувача за темою дисертації:

1. Смірнов І.С., Кодинець А.О. Порівняння захисту прав інтелектуальної власності на програмне забезпечення в Україні, Європейському Союзі та Сполучених Штатах Америки // Матеріали Всеукраїнської науково-практичної конференції " "Інкорпорація та кодифікація законодавства як складові стратегії розвитку сфери інтелектуальної власності в Україні"". – Київ, 2022. – С. 235–240.
2. Смірнов І.С. Перспективи застосування технології блокчейн в управлінні правами інтелектуальної власності // Матеріали V Міжнародної науково-практичної конференції "Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об’єктів права інтелектуальної власності, трансфер технологій". – Київ, 2022. – С. 94–98.
3. Смірнов І.С. Перспективи застосування смарт-контракту як засобу забезпечення виконання зобов’язань // Юридичний науковий електронний журнал. – 2023. – № 6. – С. 189–191.
4. Смірнов І. Захист авторських прав у Web3 // Матеріали XI Всеукраїнської науково-практичної конференції молодих вчених та студентів з проблем інтелектуальної власності "Законодавство України у сфері інтелектуальної власності та його правозастосування: національна, європейські та міжнародні виміри", 12 жовтня 2023 року. – Київ, 2023. – С. 122–127.
5. Смірнов Ігор. Правове регулювання та етичні виклики використання штучного інтелекту для управління блокчейн-мережами // Матеріали міжнародної

науково-практичної конференції "Правове регулювання цифрової економіки та штучного інтелекту: національний та міжнародний виміри". – Київ, 2023. – С. 221–226.

6. Смірнов І.С. Роль блокчейн-технологій у запобіганні недобросовісній конкуренції // Матеріали Всеукраїнської науково-практичної конференції "Захист від недобросовісної конкуренції в умовах євроінтеграції та цифрової трансформації", 31 травня 2024 року. – Київ, 2024. – С. 131–136.
7. Смірнов І. Регулювання конфіденційності у епоху блокчейну: правові аспекти та перспективи // Юридичний науковий електронний журнал. – Київ, 2024. – 5 с. (№ 5 за 2024 р.).
8. Смірнов Ігор. Перспективи патентування блокчейн-технологій // Матеріали XII Всеукраїнської науково-практичної конференції молодих вчених та студентів з проблем інтелектуальної власності "Законодавство України у сфері інтелектуальної власності та його правозастосування: національні, європейські та міжнародні виміри", 11 жовтня 2024 року. – Київ, 2024. – С. 160–164.
9. Смірнов Ігор. Децентралізація як ключовий елемент блокчейну та його правові наслідки // Матеріали науково-практичної конференції "Україна в умовах соціальної та цифрової трансформації: шляхи до сталого розвитку та повоєнної відбудови", 22 листопада 2024 року. – Київ, 2024. – С. 209–215.
10. Смірнов Ігор. Трансформація інформаційних відносин в еру блокчейн-технологій // KELM (Knowledge, Education, Law, Management). – 2025. – № 1(69). – DOI https://doi.org/10.51647/kelm.2025.1.30.
11. Смірнов Ігор С. Трансформація змісту інформаційних відносин у блокчейн-середовищі: правові та технологічні аспекти // Юридичний науковий електронний журнал. – 2025. – № 5.

A N N O T A T I O N

Smirnov I.S. Legal Regulation of Information Relations Arising in Connection with Blockchain Technology. – A Qualification Scholarly Work (Manuscript).

A thesis was submitted for the Doctor of Philosophy in Law degree (speciality 081 "Law"). – Taras Shevchenko National University of Kyiv, Kyiv, 2026.

This dissertation presents a comprehensive study of the legal framework governing information relations emerging through the application of blockchain technology in the contemporary digital environment. The need for enhanced legislative regulation stems from the rapid proliferation of decentralized networks, their multidimensional impact on economic, legal, and social domains, and the formation of novel legal mechanisms for managing virtual assets, including cryptocurrencies, tokens, and smart contracts.

The first chapter provides a detailed theoretical and legal analysis of blockchain technology as a unique phenomenon of the modern information era. Considering the stages of distributed ledger development, the study examines the fundamental principles of blockchain (decentralization, immutability of records, cryptographic protection) and their direct influence on the legal relations formed within this technological framework. The research demonstrates that understanding blockchain's essence and related information processes enables the identification of the legal status of participants (users, miners, developers, regulators), their mutual rights and obligations, and clarifies the role of the informational component in digital transactions.

The second chapter focuses on the civil law aspects of blockchain technologies, particularly exploring the legal nature of virtual assets (cryptocurrencies, tokens, NFTs). The author proposes a classification of virtual assets based on their functional purpose, economic substance, liquidity, and potential as payment instruments. Special attention is devoted to smart contracts: the theoretical foundations for considering them as an electronic form of legal transaction are substantiated, wherein contractual terms are encoded and execution occurs automatically. The research reveals that the absence of specialized legislative regulation for smart contracts creates legal risks related to determining the parties' intent, mechanisms for code modification, and dispute resolution. The study proves that smart contracts can become an effective tool for ensuring the fulfillment of obligations across various domains—from financial operations to intellectual property management.

The third chapter concentrates on international legal experience and mechanisms for protecting the rights of participants in blockchain-based information relations. A

comparative analysis of regulatory models for cryptocurrencies and decentralized finance across different jurisdictions is conducted: the European Union (directives, MiCA regulation), the United States (SEC, CFTC approaches), China (restrictions on crypto activities alongside development of a state digital yuan), as well as Switzerland, Singapore, and Japan. The research establishes that the lack of harmonized international standards in the blockchain sphere creates legal norm conflicts, complicates cross-border operations, and requires a more active role from international organizations (FATF, ISO, WIPO). The study explores intellectual property protection in Web3, regulation of NFTs and digital content platforms, and addresses privacy challenges, including conflicts with GDPR's "right to be forgotten" requirements.

The fourth chapter is dedicated to perspectives for improving the legal regulation of blockchain technologies in Ukraine. The current state of the regulatory framework is analyzed, including the Law of Ukraine "On Virtual Assets," subordinate legislation, and the role of regulatory bodies. Recommendations are formulated for implementing "regulatory sandboxes" for blockchain projects, enabling the testing of innovative solutions with minimal risks. The research substantiates the feasibility of developing the smart government concept through blockchain integration into state registries, public procurement, and electronic voting. The study demonstrates that incorporating decentralized technologies into the public sector will contribute to enhanced transparency, reduced corruption risks, and optimized administrative procedures.

The scientific novelty lies in the comprehensive, interdisciplinary analysis of blockchain as a legal phenomenon that combines elements of information, civil, financial, and international law. The dissertation systematizes concepts of transforming information resource management through decentralization and proposes approaches to the legal qualification of virtual assets. For the first time in Ukrainian legal doctrine, blockchain is examined not merely as a tool for cryptocurrency operations but also as a mechanism for protecting intellectual property rights, ensuring transparency in business processes, and modernizing public administration.

The practical significance of the results lies in their potential application in developing normative legal acts, preparing draft laws on virtual assets and smart contracts, and

improving the Civil Code of Ukraine. Additionally, the proposed concepts can be utilized in forming specialized educational disciplines and professional development programs in digital law, IT law, and intellectual property.

The conclusion states that implementing blockchain technologies in Ukraine can serve as a catalyst for digital transformation, ensuring the formation of transparent and predictable market functioning rules. At the same time, fully realizing blockchain's potential requires improving legislative mechanisms for protecting participants' rights, regulating the activities of miners and virtual asset operators, and implementing effective tools against fraud and illegal income legalization. It is important to consider international experience, particularly the EU regulatory approaches, FATF recommendations, and practices of leading countries, to ensure compatibility of legal systems and attract foreign investment into domestic blockchain infrastructure.

Thus, this dissertation reveals the legal nature and operational mechanisms of information relations in distributed networks, defines the place and role of blockchain technology in the modern legal system, and offers a complex of legislative and practical recommendations for forming an effective regulatory framework. The obtained results create a foundation for further scientific research in digital technologies, intellectual property, e-commerce, and legal support for innovations.

Keywords: *blockchain technology, information relations, legal regulation, virtual assets, cryptocurrency, smart contracts, NFT, protection of intellectual property rights, copyright, information and communication technologies, digital environment, adaptation of legislation to the EU.*

List of the Applicant's Publications on the Dissertation Topic:

1. Smirnov I.S. Comparison of Intellectual Property Rights Protection for Software in Ukraine, the European Union, and the United States // Materials of the All-Ukrainian Research and Practical Conference "Incorporation and Codification of Legislation as Components of the Strategy for the Development of the Intellectual Property Sphere in Ukraine". – Kyiv, 2022. – pp. 235–240.
2. Smirnov I.S. Prospects of Using Blockchain Technology in the Management of Intellectual Property Rights // Materials of the 5th International Research and

Practical Conference "Project Management. Prospects for the Development of Project and Neuromanagement, Information Management Technologies, Creation and Use of Intellectual Property Rights, Technology Transfer". – Kyiv, 2022. – pp. 94–98.

3. Smirnov I.S. Prospects of Using a Smart Contract as a Means of Ensuring the Fulfillment of Obligations // Jurydychnyi Naukovyi Elektronnyi Zhurnal (Legal Scholarly E-Journal). – 2023. – No. 6. – pp. 189–191.
4. Smirnov I. Copyright Protection in Web3 // Materials of the 11th All-Ukrainian Research and Practical Conference of Young Scientists and Students on Intellectual Property Issues "Legislation of Ukraine in the Field of Intellectual Property and Its Enforcement: National, European and International Dimensions", October 12, 2023. – Kyiv, 2023. – pp. 122–127.
5. Smirnov Ihor. Legal Regulation and Ethical Challenges of Using Artificial Intelligence to Manage Blockchain Networks // Materials of the International Research and Practical Conference "Legal Regulation of the Digital Economy and Artificial Intelligence: National and International Dimensions". – Kyiv, 2023. – pp. 221–226.
6. Smirnov I.S. The Role of Blockchain Technologies in Preventing Unfair Competition // Materials of the All-Ukrainian Research and Practical Conference "Protection Against Unfair Competition in the Conditions of European Integration and Digital Transformation", May 31, 2024. – Kyiv, 2024. – pp. 131–136.
7. Smirnov I. Regulation of Privacy in the Era of Blockchain: Legal Aspects and Prospects // Jurydychnyi Naukovyi Elektronnyi Zhurnal (Legal Scholarly E-Journal). – Kyiv, 2024. – 5 p. (No. 5 for 2024).
8. Smirnov Ihor. Prospects for Patent Protection of Blockchain Technologies // Materials of the 12th All-Ukrainian Research and Practical Conference of Young Scientists and Students on Intellectual Property Issues "Legislation of Ukraine in the Field of Intellectual Property and Its Enforcement: National, European and International Dimensions", October 11, 2024. – Kyiv, 2024. – pp. 160–164.
9. Smirnov Ihor. Decentralization as a Key Element of Blockchain and Its Legal Implications // Materials of the Research and Practical Conference "Ukraine in the

Conditions of Social and Digital Transformation: Ways to Sustainable Development and Post-War Recovery", November 22, 2024. – Kyiv, 2024. – pp. 209–215.

10. Smirnov Ihor. Transformation of information relations in the era of blockchain technologies // KELM (Knowledge, Education, Law, Management). – 2025. – No. 1(69). – DOI https://doi.org/10.51647/kelm.2025.1.30.

11. Smirnov Ihor S. Transformation of the Content of Information Relations in the Blockchain Environment: Legal and Technological Aspects // Jurydychnyi Naukovyi Elektronnyi Zhurnal (Legal Scholarly E-Journal). – 2025. – No. 5.

З М І С Т

П Е Р Е Л І К У М О В Н И Х П О З Н А Ч Е Н Ь Т А С К О Р О Ч Е Н Ь

Абревіатури, що пов’язані з державами та міжнародними організаціями:

1. США – Сполучені Штати Америки
2. ЄС – Європейський Союз
3. ООН – Організація Об’єднаних Націй
4. СОТ – Світова організація торгівлі (WTO)

Абревіатури, що стосуються регулювання, стандартів і моніторингу:

1. FATF (Financial Action Task Force) – Міжнародна група з протидії відмиванню коштів
2. ISO (International Organization for Standardization) – Міжнародна організація зі стандартизації
3. WIPO (World Intellectual Property Organization) – Всесвітня організація інтелектуальної власності
4. MiCA (Markets in Crypto-Assets) – Регламент ЄС про ринки криптоактивів
5. AML (Anti-Money Laundering) – протидія відмиванню коштів
6. KYC (Know Your Customer) – процедура ідентифікації клієнтів
7. CFT (Combating the Financing of Terrorism) - протидія фінансуванню тероризму
8. SEC (Securities and Exchange Commission) – Комісія з цінних паперів і бірж
9. CFTC (Commodity Futures Trading Commission) – Комісія з торгівлі ф’ючерсами
10. IOSCO (International Organization of Securities Commissions) - Міжнародна організація комісій з цінних паперів
11. FSB - (Financial Stability Board) - Рада з фінансової стабільності
12. MAS (Monetary Authority of Singapore) - Валютне управління Сінгапуру

Абревіатури, що позначають технології та явища у сфері блокчейну:

1. DAO (Decentralized Autonomous Organization) – децентралізована автономна організація, функціонує на основі смарт-контрактів
2. DeFi (Decentralized Finance) – децентралізовані фінансові сервіси

3. NFT (Non-Fungible Token) – невзаємозамінний токен, унікальний цифровий актив, який не може бути замінений іншим подібним активом
4. ICO (Initial Coin Offering) – первинна пропозиція монет (токенів)
5. IEO (Initial Exchange Offering) – первинна пропозиція монет (токенів) на біржі
6. STO (Security Token Offering) – пропозиція токенів, прирівняних до цінних паперів
7. CBDC (Central Bank Digital Currency) – цифрова валюта центрального банку
8. DApps (Decentralized Applications) – децентралізовані додатки
9. P2P (peer-to-peer) - модель мережевої взаємодії, де всі учасники мають рівні права та можуть безпосередньо обмінюватися даними без центрального сервера
10. PoW (Proof of Work) - механізм консенсусу, що базується на вирішенні складних математичних задач.
11. PoS (Proof of Stake) - механізм консенсусу, що базується на блокуванні токенів.
12. DPoS (Delegated Proof of Stake) - делегований механізм консенсусу Proof of Stake.
13. L1 (Layer 1) - основний рівень блокчейну.
14. L2 (Layer 2) - другий рівень блокчейну, що забезпечує масштабованість. Це додатковий протокол, розташований над Layer 1, який вирішує проблеми масштабованості, дозволяючи проводити транзакції поза основним ланцюгом та періодично звіряти результати з основним блокчейном, що значно підвищує швидкість та знижує вартість обробки транзакцій.
15. VASP – абревіатура постачальників послуг з віртуальними активами у США (Virtual Asset Service Provider), по тексту також відповідає CASP у MiCA (Crypto-Asset Service Provider).

Абревіатури й скорочення у правовому та регуляторному полі України:

1. НБУ – Національний банк України
2. НКЦПФР – Національна комісія з цінних паперів та фондового ринку
3. Мінцифри – Міністерство цифрової трансформації України

4. Дія (у контексті «Дія.City») – цифровий бренд і платформа держпослуг в Україні
5. ЗУ – Закон України
6. ЦКУ – Цивільний кодекс України
7. ПКУ – Податковий кодекс України

Інші поширені скорочення в тексті:

1. GDPR (General Data Protection Regulation) – Загальний регламент ЄС із захисту даних
2. SRO (Self-Regulatory Organization) – саморегульована організація
3. USDT (Tether) - стейблкоїн, прив'язаний до долара США
4. USDC (USD Coin) - стейблкоїн, прив'язаний до долара США
5. IoT (Internet of Things) - система взаємопов'язаних обчислювальних пристроїв, що можуть збирати та обмінюватися даними через мережу без прямого втручання людини

Р О З ' Я С Н Е Н Н Я К Л Ю Ч О В И Х П О Н Я Т Ь

Для забезпечення термінологічної чіткості та послідовності дослідження, визначимо ключові поняття, що будуть використовуватися в роботі:

1. Блокчейн (blockchain) – розподілена база даних, що зберігає впорядкований ланцюжок записів (блоків), який постійно довшає. Кожен блок містить часову мітку, хеш попереднього блоку та дані транзакцій.
2. Криптографічний хеш – результат перетворення вхідних даних будь-якого розміру в бітовий рядок встановленої довжини за допомогою криптографічної хеш-функції.
3. Консенсус – механізм досягнення узгодженості щодо стану мережі між її учасниками.

Суб'єкти блокчейн-відносин:

1. Вузол (node) – учасник мережі, що зберігає повну копію блокчейну та бере участь у валідації транзакцій.
2. Майнер – учасник мережі, який забезпечує формування нових блоків у системах з механізмом Proof of Work.
3. Валідатор – учасник мережі, який підтверджує транзакції в системах з механізмом Proof of Stake.

Об'єкти та інструменти:

1. Віртуальний актив – цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати, і який може використовуватися для платіжних або інвестиційних цілей.
2. Токен – цифрова одиниця обліку в межах блокчейн-платформи, яка представляє актив або корисність.

Правові механізми:

1. Смарт-контракт – програмний код, що функціонує в блокчейн-середовищі та автоматично виконує визначені умови.
2. Цифрова ідентифікація – процес підтвердження особи користувача в блокчейн-мережі через криптографічні методи.
3. Цифровий підпис – криптографічний метод, що дозволяє підтвердити автентичність та цілісність цифрових повідомлень або документів.

Регуляторні аспекти:

1. Регуляторна пісочниця (sandbox) – спеціальний режим, що дозволяє тестувати інноваційні фінансові продукти та послуги під наглядом регулятора.

Специфічні концепції Web3:

1. Метавсесвіт (metaverse) – віртуальний простір, де можуть взаємодіяти користувачі та цифрові активи.
2. White Paper - документ, що містить детальний опис блокчейн-проєкту, включаючи його технічні характеристики, економічну модель та план розвитку
3. Utility-токен - токен, що надає доступ до певних сервісів або послуг
4. Security-токен - токен, що представляє права на традиційні фінансові активи
5. Стейблкоїн - криптовалюта, вартість якої прив'язана до традиційних активів
6. Нативний токен - токен, який є основною криптовалютою певного блокчейну
7. Gas fees - плата за обчислювальні ресурси в мережі Ethereum, часто термін використовується як плата за за дії в інших блокчейнах.
8. Оракули (oracles) - механізми введення даних із зовнішнього світу в блокчейн-середовище, що забезпечують доступ смарт-контрактів до інформації поза блокчейном.
9. Криптографічні ключі - спеціальні дані, що використовуються для шифрування і дешифрування інформації, а також підтвердження власності на віртуальні активи (включають приватні та публічні ключі).

10. Холодні гаманці/сховища - спосіб зберігання криптографічних ключів без підключення до інтернету, що забезпечує підвищений рівень безпеки для віртуальних активів.
11. Інтероперабельність (interoperability) - здатність різних блокчейн-мереж до взаємодії та обміну даними.
12. Крос-чейн взаємодія (cross-chain interaction) - технології та протоколи, що забезпечують передачу даних та активів між різними блокчейн-мережами.
13. Цифровий депозитарій - спеціалізована установа для обліку, зберігання та обслуговування операцій з цифровими активами.
14. Глибокий захист (defense in depth) - стратегія забезпечення безпеки шляхом використання багаторівневої системи захисних механізмів.
15. Технологічна нейтральність - принцип регулювання, що фокусується на функціональному призначенні технології та її правових наслідках, а не на технічних характеристиках.
16. Маркет-мейкери - учасники ринку, що забезпечують ліквідність шляхом одночасного виставлення заявок на купівлю та продаж активів.
17. Мультипідписні гаманці (multisig wallets) - гаманці віртуальних активів, що вимагають кілька підписів (ключів) для авторизації транзакції, підвищуючи рівень безпеки.

Ці терміни формують концептуальну основу дослідження та будуть використовуватися в наступних розділах при аналізі конкретних аспектів правового регулювання блокчейн-технологій. Їх чітке визначення необхідне для забезпечення однозначного розуміння та коректної інтерпретації правових норм та механізмів регулювання.

В С Т У П

Обґрунтування вибору теми дослідження. Тема розвивається на перетині інформаційного права, права інтелектуальної власності, цивільного права, фінансового права та міжнародного приватного права, що зумовлено міждисциплінарною природою блокчейн-технологій і широким спектром їх застосування. В умовах активної цифровізації економіки та державного управління, формування глобальних комерційних мереж і децентралізованих фінансових сервісів (далі також – "DeFi"), а також розвитку smart government та електронного врядування необхідність дослідження правових засад блокчейну набуває особливої актуальності. Дослідження спирається на аналіз сучасної наукової літератури та публікації автора, в яких було розпочато критичний аналіз чинних правових підходів і виявлено проблематику відсутності уніфікованого термінологічного апарату, фрагментованості регуляторних норм і браку узгоджених методологічних рекомендацій для правозастосування.

Мета та завдання дослідження. Метою дисертації є формування комплексної концепції правового регулювання інформаційних відносин, що виникають у зв'язку з використанням блокчейн-технології, з розробкою науково обґрунтованих пропозицій щодо вдосконалення вітчизняного законодавства й імплементації передових міжнародних практик.

Для досягнення поставленої мети були визначені такі основні завдання:

1. Дослідити теоретичні засади та характерні риси блокчейн-технології як інформаційного феномену;
2. Розкрити структуру та сутність інформаційних відносин у блокчейн-середовищі, виокремивши їх суб'єктів, об'єкти та зміст;
3. Проаналізувати цивільно-правову природу віртуальних активів, смарт-контрактів і механізмів захисту прав учасників блокчейн-відносин;
4. Систематизувати міжнародний досвід правового регулювання криптовалют, токенів, NFT та визначити можливості адаптації закордонних моделей до національного законодавства;

5. Розробити пропозиції щодо вдосконалення нормативно-правової бази України у сфері блокчейн-технологій, включаючи концепції "регуляторних пісочниць" та автоматизованих платформ державних послуг;
6. Обґрунтувати потенціал блокчейну для захисту прав інтелектуальної власності, забезпечення прозорості та протидії недобросовісній конкуренції.

Об’єкт і предмет дослідження. Об'єктом дослідження є комплекс правовідносин, що формуються в процесі створення, обігу та використання інформації в децентралізованих блокчейн-мережах, а також правові механізми захисту учасників таких відносин.

Предметом дослідження виступають норми законодавства України, закордонних країн і міжнародні акти, наукові праці, матеріали судової практики та публікації, що стосуються правової природи блокчейну, віртуальних активів, смарт-контрактів та споріднених аспектів інформаційного права.

Методи дослідження. Для отримання правдивих і всебічних результатів застосовано комплекс наукових методів:

- Історико-правовий – для виявлення етапів розвитку блокчейну, його концептуальних прототипів і еволюції підходів до регулювання технологій.
- Порівняльно-правовий – дозволив зіставити законодавство й правозастосовну практику різних країн щодо блокчейн-технологій, виявити спільні тенденції та відмінності, оцінити ефективність регуляторних моделей.
- Системний – забезпечив розгляд блокчейну як цілісної системи, що інтегрує технологічні, соціальні та економічні компоненти, а також правову регламентацію та взаємодію суб'єктів.
- Формально-логічний – сприяв уточненню понятєвого апарату ("віртуальні активи", "криптовалюта", "смарт-контракт" тощо) та подоланню термінологічних колізій.
- Догматичний (формально-юридичний) – застосовано для тлумачення нормативних положень, визначення співвідношення між загальними нормами законодавства та спеціальними вимогами до обігу віртуальних активів.

- Правового прогнозування – використано для аналізу перспектив розвитку блокчейн-технологій та формулювання пропозицій з удосконалення нормативно-правової бази.

Обґрунтування вибору цих методів полягає в необхідності комплексного та багатовимірного підходу до дослідження блокчейну, що поєднує технологічний аспект із правовим регулюванням. Застосування порівняльно-правового та системного методів забезпечило широкий аналіз законодавчих практик на міжнародному рівні та сформувало підґрунтя для розробки пропозицій щодо їх імплементації в національне законодавство.

Наукова новизна отриманих результатів. Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших в українській правовій науці комплексних досліджень правового регулювання інформаційних відносин, що виникають у зв'язку із застосуванням блокчейн-технології. У результаті проведеного дослідження:

Вперше:

1) визначено дуалістичну правову природу блокчейн-технології як одночасно інфраструктури, що забезпечує децентралізоване зберігання та передачу даних, і системи взаємодій, заснованої на нових механізмах довіри та координації, що зумовлює необхідність комплексного правового регулювання на перетині інформаційного права (регулювання обігу даних у децентралізованих мережах), цивільного права (правочини, договори, власність на віртуальні активи), фінансового права (обіг криптовалют, токенів) та міжнародного приватного права (транскордонні операції);

2) систематизовано на основі функціонального призначення та правового режиму типологію об'єктів інформаційних відносин у блокчейн-середовищі, що включає: смарт-контракти як програмні об'єкти; цифрові активи як особливу форму інформаційних ресурсів з економічною цінністю; NFT як специфічний об'єкт із подвійною природою; інформаційні об'єкти спеціального призначення, що дозволяє

визначити відповідний правовий режим для кожної категорії об'єктів та уникнути застосування неадекватних регуляторних підходів;

3) виявлено та охарактеризовано три типи регуляторних підходів до блокчейн-технологій у міжнародній практиці: відкрито-ліберальний, помірковано-регульований та жорстко-рестриктивний, з обґрунтуванням найбільшої ефективності першого типу;

4) запропоновано три сценарії міжнародної гармонізації регулювання блокчейн-технологій: поступова конвергенція, регіональна гармонізація та фрагментація з "мостами", з обґрунтуванням найбільшої імовірності другого сценарію як такого, що дозволяє поєднати переваги уніфікації в межах регіональних блоків (ЄС, АСЕАН) зі збереженням специфіки національних правових систем, що відповідає сучасним тенденціям регіоналізації міжнародного права;

5) виявлено специфіку механізму консенсусу як правового явища у блокчейн-середовищі, що полягає у заміні традиційного нотаріального засвідчення чи судового підтвердження автентичності інформації на розподілену систему верифікації через алгоритмічні протоколи (Proof of Work, Proof of Stake), що створює нову парадигму підтвердження достовірності правочинів без участі довірених третіх осіб;

Удосконалено:

1) класифікацію договорів з віртуальними активами за функціональним призначенням та правовою природою, що охоплює договори купівлі-продажу, договори про надання послуг, інвестиційні договори, ліцензійні договори та договори про створення й використання токенізованих активів;

2) систему способів забезпечення виконання зобов'язань у блокчейн-середовищі, включаючи смарт-контракти з функцією умовного виконання, мультипідписні транзакції, токенізацію активів та механізми цифрового депонування;

3) концепцію трансформації права власності на віртуальні активи через призму криптографічних ключів, де володіння реалізується через контроль над ключами, користування через здійснення транзакцій, а розпорядження через передачу прав;

4) положення про інститут цивільно-правової відповідальності у блокчейн-відносинах шляхом виділення специфічних підстав відповідальності (порушення

умов смарт-контракту, неправомірне використання криптографічних ключів, недотримання протоколів мережі) та механізмів розподілу ризиків в умовах незворотності транзакцій і автономії учасників децентралізованих систем;

Набули подальшого розвитку:

1) положення про трансформацію принципів свободи, достовірності та захисту інформації в блокчейн-середовищі, де свобода набуває нового змісту через неможливість обмеження доступу, достовірність забезпечується консенсусом, а захист розподіленою системою безпеки;

2) положення про адаптацію принципу автономії волі до цифрового середовища, де волевиявлення реалізується через взаємодію з програмним кодом та криптографічними механізмами, що призводить до трансформації традиційних інститутів форми правочину (фіксація волі через цифровий підпис), його дійсності (неможливість оспорення після виконання смарт-контракту) та створює необхідність розробки спеціальних норм щодо визначення моменту виникнення правових наслідків у автоматизованих правочинах;

3) положення про неможливість визнання смарт-контрактів суб'єктами правовідносин, оскільки вони є лише інструментом автоматизованого виконання умов, на відміну від децентралізованих автономних організацій (DAO - Decentralized Autonomous Organizations), які можуть набувати ознак правосуб'єктності за умови наявності механізмів колективного прийняття рішень учасниками через голосування токенами (governance tokens), можливості укладення договорів від імені організації та наявності відокремленого майна у формі пулу віртуальних активів, що розвиває теорію юридичної особи у контексті децентралізованих цифрових утворень;

Особистий внесок здобувача. Дисертаційна робота виконана автором особисто. У дослідженні не використано ідей чи розробок, що належать співавторам публікацій. Усі наукові праці, опубліковані за темою дисертації, створені самостійно (або у співавторстві з науковим керівником, де внесок здобувача є визначальним). Кожен сформульований науковий висновок та методологічна пропозиція ґрунтуються на самостійному аналізі законодавчих актів, наукових публікацій і практичних матеріалів, що підтверджено відповідними посиланнями в тексті дисертації.

Апробація матеріалів дисертації. Основні положення та висновки дисертаційного дослідження було представлено та обговорено на таких науково-практичних заходах:

- V Міжнародна науково-практична конференція "Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об'єктів права інтелектуальної власності, трансфер технологій" (Київ, 2022);
- XI Всеукраїнська науково-практична конференція молодих вчених та студентів з проблем інтелектуальної власності "Законодавство України у сфері інтелектуальної власності та його правозастосування: національна, європейські та міжнародні виміри" (Київ, 2023);
- Міжнародна науково-практична конференція "Правове регулювання цифрової економіки та штучного інтелекту: національний та міжнародний виміри" (Київ, 2023);
- Всеукраїнська науково-практична конференція "Захист від недобросовісної конкуренції в умовах євроінтеграції та цифрової трансформації" (2024);
- XII Всеукраїнська науково-практична конференція молодих вчених та студентів з проблем інтелектуальної власності "Законодавство України у сфері інтелектуальної власності та його правозастосування: національні, європейські та міжнародні виміри" (Київ, 2024);

За результатами виступів отримано позитивні відгуки, змістовні пропозиції та підтвердження актуальності дослідження.

Практичне значення отриманих результатів. Результати дослідження мають широке практичне застосування і можуть бути використані:

1. У нормотворчій діяльності – для розробки законопроєктів, що визначають статус віртуальних активів, умови укладення й виконання смарт-контрактів, механізми регулювання блокчейну, а також для вдосконалення положень Цивільного кодексу України та законодавства про електронні правочини.

2. У правозастосовній практиці – як методичні рекомендації для суддів, нотаріусів, державних реєстраторів та інших юристів при вирішенні спорів, пов'язаних із блокчейном, або засвідченні цифрових правочинів.
3. У діяльності органів державного управління – для підвищення ефективності реєстрів, протидії корупції, оптимізації процедур, розвитку врядування.
4. У бізнес-середовищі – при формуванні корпоративних політик і систем управління віртуальними активами, створенні децентралізованих платформ для торгівлі товарами, послугами, об'єктами інтелектуальної власності, а також при залученні інвестицій та емісії різних видів токенів.
5. В освітньому процесі – як теоретична основа для спеціалізованих курсів з цифрового права, інформаційного права та інтелектуальної власності в цифрову епоху. Матеріали дисертації можуть бути інтегровані до методичних посібників і навчальних програм юридичних спеціальностей.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконане в рамках індивідуальної наукової тематики, не пов'язаної з грантами чи державними науковими програмами.

Структура та обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації – 226 сторінок комп'ютерного тексту (11 авторських аркушів). Структура розроблена з урахуванням логічної послідовності вирішення завдань, сформульованих у вступі:

- Розділ 1: Теоретико-правові засади блокчейн-технології як об'єкта правового регулювання
- Розділ 2: Цивільно-правові аспекти регулювання блокчейн-відносин
- Розділ 3: Міжнародний досвід правового регулювання блокчейн-технологій
- Розділ 4: Напрямки вдосконалення правового регулювання блокчейн-технологій в Україні

Кожен розділ поділяється на підрозділи з відповідною нумерацією. Список використаних джерел сформовано згідно з національним стандартом бібліографічного опису (ДСТУ 8302:2015).

Таким чином, структура дисертаційної роботи побудована послідовно для комплексного розкриття сутності блокчейну, аналізу міжнародного та вітчизняного досвіду регулювання, дослідження цивільно-правових аспектів та формулювання науково обґрунтованих пропозицій щодо вдосконалення правової бази України.

Р О З Д І Л 1. Інформаційні відносини у сфері блокчейн-технологій

1.1. Теоретико-правові основи блокчейн-технології

Дослідження інформаційних відносин у сфері блокчейн-технології потребує особливого методологічного підходу, що враховує специфіку децентралізованих взаємодій. Ключовими аспектами дослідження є: розгляд блокчейну як комплексного інформаційно-правового феномену, де технічні характеристики пов'язані з правовими наслідками [1]; аналіз трансформації традиційних інформаційних прав та обов'язків у децентралізованому середовищі [2]; вивчення нових форм фіксації та передачі інформації, що базуються на криптографічних механізмах та консенсусі [3].

Методологічна основа дослідження інформаційних відносин у сфері блокчейн-технологій базується на комплексному застосуванні різних наукових методів:

- Історико-правовий метод застосовується в підрозділі 1.1 для аналізу еволюції блокчейн-технології та трансформації підходів до її регулювання.
- Системний метод є основним для підрозділу 1.1 при дослідженні технічних аспектів як єдиної системи взаємопов'язаних елементів.
- Формально-логічний метод використовується в підрозділі 1.2 для класифікації суб'єктів та об'єктів.
- Порівняльно-правовий метод застосовується наскрізно для зіставлення різних підходів до регулювання.
- Методи аналізу та синтезу використовуються в підрозділі 1.3 для дослідження змісту правовідносин.

У межах цього дослідження терміни "блокчейн", "блокчейн-технологія" та "технологія блокчейн" використовуються як синоніми для позначення технології розподіленого реєстру, що забезпечує децентралізоване зберігання та передачу інформації [4]. Аналогічно, терміни "смарт-контракт", "розумний контракт" та "програмований контракт" вживаються як рівнозначні поняття для позначення програмного коду, що автоматично виконує визначені умови в блокчейн-середовищі

[5]. Таке використання синонімічних термінів відповідає усталеній науковій практиці та дозволяє уникнути надмірних повторів при збереженні точності викладу.

Одним із фундаментальних прав, що визначають засади формування інформаційних відносин, є гарантована Конституцією України свобода кожного збирати, зберігати, використовувати й поширювати інформацію в будь-який спосіб на власний вибір [6]. Аналогічну норму містить і ЦКУ, в якому закріплено право фізичної особи на вільне збирання та використання інформації [7]. Ці конституційно-цивільні приписи набувають особливого значення у "цифрову епоху", коли традиційні підходи до обігу даних зазнають істотних змін [8].

У контексті дослідження блокчейн-технології особливого значення набуває термінологічний апарат інформаційного права, який потребує уточнення та адаптації до нових технологічних реалій [9]. Ключовими поняттями виступають:

- Інформація в блокчейн-середовищі — це сукупність відомостей про транзакції, активи, права та обов'язки учасників, що набуває змістовного значення в контексті конкретних правовідносин та має юридичне значення [10].
- Дані в контексті блокчейну — це формалізовані цифрові записи, що містять відомості про транзакції, криптографічні підписи та метадані, які зберігаються в розподіленому реєстрі у вигляді послідовності блоків [11].
- Блокчейн-транзакція — інформаційний запис про передачу цифрових активів або даних між учасниками мережі, що підтверджується криптографічними методами та зберігається у розподіленому реєстрі [12].
- Розподілений реєстр — децентралізована база даних, що підтримується та оновлюється незалежними вузлами мережі на основі механізмів консенсусу [13].

Блокчейн (англ. blockchain - "ланцюг блоків") є інноваційною технологією розподіленого реєстру, що забезпечує зберігання та передачу даних через систему пов'язаних блоків інформації. Ця технологія функціонує без центру управління, що робить її важливою для розвитку сучасних інформаційних відносин [4].

Перші спроби створити надійний і невразливий до підроблення механізм фіксації даних датуються початком 1990-х років. Так, С. Хабер і В. Сторнетта запропонували систему "timestamping", що унеможливлювала приховане редагування електронних документів. Ця концепція лягла в основу майбутніх децентралізованих реєстрів.

Кардинальний прорив відбувся у 2008 році, коли під псевдонімом Сатоші Накамото з'явилася стаття "Bitcoin: A Peer-to-Peer Electronic Cash System" [11]. У ній обґрунтовано ідею створення системи, де інформація про транзакції фіксується в розподіленій базі даних, а її достовірність перевіряється всіма учасниками мережі без залучення центрального органу. Поступово технологія вийшла за межі криптовалютних проєктів, поширившись на управління цифровими активами, інтелектуальними правами, публічні реєстри та документообіг [12].

За даними дослідження Deloitte's 2021 Global Blockchain Survey, технологія отримала найбільше впровадження у фінансовому секторі (45% від усіх впроваджень), логістиці (15%), охороні здоров'я (12%) та державному управлінні (10%). При цьому основними перешкодами для впровадження залишаються регуляторна невизначеність (43%) та технологічна складність (38%) [14].

Динаміка розвитку блокчейн-технологій демонструє стрімке зростання:

- Ринкова капіталізація криптоактивів збільшується.
- Інвестиції у блокчейн-інфраструктуру зростають.
- Кількість активних блокчейн-гаманців збільшилась з 10 мільйонів у 2016 році до понад 500 мільйонів у 2024 році.
- Зростає обсяг транзакцій у публічних блокчейнах.
- Обсяг ринку DeFi-сектору зростає [15].

Блокчейн характеризується особливими рисами.

Децентралізація передбачає, що дані зберігаються не на одному сервері, а розподілені між вузлами мережі. Це мінімізує залежність від окремої установи, підвищуючи стійкість системи та зменшуючи ризики цензури [3].

Незмінність записів означає, що кожен блок містить криптографічний "хеш" попереднього блоку, а для зміни інформації потрібно змінювати всі наступні блоки.

У великих мережах це практично нездійсненно, адже потребує колосальної обчислювальної потужності й погодження більшості учасників [11].

Розподілена архітектура, де учасники зберігають повну або часткову копію реєстру, а "оновлення" блоків відбувається одночасно на всіх вузлах після підтвердження за алгоритмом консенсусу [10].

Окрім технічних характеристик, блокчейн створює нові форми довіри та співпраці між учасниками, що трансформує традиційні моделі правового регулювання [16].

Міждисциплінарний характер блокчейн-технології проявляється у взаємозв'язку інформаційного права з іншими галузями права та науковими дисциплінами:

Взаємодія з цивільним правом виявляється у трансформації інститутів власності та договірного права під впливом цифровізації. Блокчейн створює нові форми фіксації та передачі прав, що вимагає переосмислення чинних конструкцій [17].

У контексті фінансового права блокчейн-технологія впливає на розуміння природи грошей та платіжних систем. Виникають нові форми фінансових інструментів, що потребують специфічних механізмів регулювання [18].

Взаємозв'язок з адміністративним правом проявляється у питаннях державного регулювання та контролю за блокчейн-системами. Уваги потребує трансформація механізмів надання адміністративних послуг та ведення державних реєстрів [19].

У сфері кримінального права та криміналістики блокчейн створює нові виклики щодо ідентифікації правопорушень та збору доказів. Водночас технологія надає нові інструменти для протидії кіберзлочинності [20].

Технічні науки забезпечують розуміння механізмів функціонування блокчейну, зокрема криптографічних протоколів та алгоритмів консенсусу. Це критично важливо для формування адекватних правових механізмів регулювання [21].

Економічна наука досліджує вплив блокчейну на трансформацію бізнес-моделей та фінансових відносин. Виникають нові форми економічної взаємодії, що потребують правового осмислення [22].

Соціологічний аналіз розкриває вплив блокчейну на соціальні відносини, зокрема на формування нових моделей довіри та співпраці [23].

Такий міждисциплінарний підхід забезпечує комплексне розуміння природи інформаційних відносин у блокчейн-середовищі та дозволяє сформувати ефективні механізми їх правового регулювання.

В інформаційному суспільстві блокчейн-технологія постає не лише технічним інструментом, а й способом переосмислення правовідносин щодо даних. Юридично поняття "дані" охоплює цифрові записи, зашифровані у блоках; "інформація" ж — це змістовне значення, яке ці дані отримують, коли розкривається їхній контекст [9].

У сучасній практиці виділяють три види блокчейнів:

1. Публічні блокчейни (Bitcoin, Ethereum тощо) — відкриті для учасників, забезпечують прозорість операцій, історія транзакцій доступна для перегляду;
2. Приватні блокчейни — доступ обмежений визначеним колом учасників;
3. Консорціумні блокчейни — гібридний варіант, де доступ та управління здійснюється групою організацій (наприклад, проєкти держорганів) [4, 8].

Важливо розуміти, що блокчейн синтезує технологію з правовими підходами: фіксує "подію" (транзакцію, договір, передачу права) у розподіленому реєстрі, тим самим формуючи підстави для юридичної достовірності таких подій. Це посилює "довіру" до результатів обігу даних, оскільки вони з'являються не з волі одного центрального суб'єкта, а внаслідок досягнення консенсусу між усіма вузлами [2]. Однак при цьому виникають питання: наскільки може змінюватися чи стиратися інформація, якщо технологія передбачає незмінність і публічність? Чи не суперечить це праву на забуття (праву суб'єкта знищити свою особисту інформацію)? [24]

Застосування блокчейн-технології призводить до важливих правових наслідків:

1. Автоматизація правовідносин через смарт-контракти, що самостійно виконують умови правочинів без участі посередників [5];
2. Зміна доказування та аудиту, через незмінність дій та транзакцій [11];
3. Трансформація регуляторних підходів у різних сферах (фінанси, управління, охорона здоров'я) через специфіку функціонування розподілених реєстрів [16];
4. Розв'язання колізійних питань та конфліктів через характер технології [25].

Таким чином, блокчейн стає новим інфраструктурним рішенням для забезпечення надійного, безпечного та прозорого обміну інформацією в цифровому середовищі. Він здатен не лише прискорити процеси та скоротити транзакційні витрати, а й вплинути на глибші аспекти правової взаємодії — розмежування відповідальності, кваліфікацію віртуальних активів, захист персональних даних, забезпечення доказів у судових процесах тощо [1, 17]. Усе це формує підґрунтя для подальшого дослідження блокчейну як феномену інформаційного права та зумовлює потребу в оновленні нормативно-правової бази.

Впровадження блокчейн-технології призводить до фундаментальних змін у системі інформаційних відносин. Традиційні принципи інформаційного права, сформовані в умовах централізованих систем обробки інформації, потребують переосмислення в контексті децентралізованих технологій [1].

Принцип свободи інформації набуває нового змісту в блокчейн-середовищі. Якщо раніше він реалізовувався через доступ до централізованих баз даних та реєстрів, то тепер забезпечується технологічною архітектурою, де кожен учасник має повну копію реєстру. Це створює новий стандарт інформаційної прозорості [8, 13].

Принцип достовірності інформації трансформується від довіри до центрального адміністратора до математично обґрунтованої впевненості, що базується на криптографічних механізмах та колективній валідації даних. Це змінює саму природу довіри в інформаційних системах [3, 10].

Захист інформації еволюціонує від моделі централізованого контролю до розподіленої системи безпеки, де збереження цілісності забезпечується консенсусом мережі. Це створює виклики для традиційних механізмів інформаційної безпеки [20].

Вплив блокчейну на базові принципи інформаційного права проявляється у декількох ключових аспектах:

Принцип свободи інформації набуває нового змісту, оскільки блокчейн забезпечує не лише право на доступ до інформації, але й технічну неможливість обмеження такого доступу через розподілене зберігання даних. Водночас це створює виклики для реалізації права на забуття та видалення персональних даних [24, 26].

Принцип достовірності інформації реалізується через технологічні механізми верифікації, де правдивість даних забезпечується не авторитетом джерела, а математичними алгоритмами та колективним консенсусом. Це змінює традиційні підходи до встановлення достовірності інформації [2, 3].

Принцип рівності прав трансформується в технічну рівність, де кожен має однакові можливості для створення та верифікації інформації. Особливого значення це набуває в контексті публічних блокчейнів, де відсутні привілейовані користувачі [1, 4].

Трансформація інформаційних відносин під впливом блокчейну створює необхідність детального аналізу технічних аспектів функціонування цієї технології, оскільки саме технічні особливості визначають специфіку правового регулювання.

Аналіз загальної характеристики блокчейн-технології та її впливу на інформаційні відносини створює підґрунтя для дослідження приватно-правових аспектів у Розділі 2. Зокрема, розуміння принципів децентралізації та незмінності даних є ключовим для аналізу правової природи смарт-контрактів та віртуальних активів, а також особливостей їх регулювання в різних правових системах [5, 21].

Теоретичні засади блокчейн-технології, розглянуті в цьому підрозділі, мають безпосередній вплив на формування приватно-правових відносин, що будуть детально проаналізовані в Розділі 2. Зокрема:

- Принцип децентралізації визначає особливості укладання та виконання смарт-контрактів [5].
- Незмінність записів впливає на формування доказової бази в цивільно-правових спорах [11, 25].
- Криптографічні механізми створюють нову парадигму підтвердження прав власності на цифрові активи [27].
- Розподілений характер зберігання даних визначає специфіку відповідальності учасників [16, 23].

Розглянувши загальну характеристику блокчейн-технології, перейдемо до аналізу технічних аспектів її функціонування, які мають визначальний вплив на формування правового регулювання.

Для розуміння правової природи інформаційних відносин у блокчейні необхідно дослідити основи його функціонування. Архітектура блокчейн-мережі базується на розподіленій системі вузлів, які спільно підтримують єдиний реєстр транзакцій [3]. Структурно блокчейн складається з вузлів (учасників мережі), блоків (структурних одиниць з інформацією) та транзакцій (записів про передачу даних) [4, 21].

Ключовим елементом функціонування блокчейну є механізми досягнення консенсусу, що забезпечують узгодженість даних між усіма учасниками мережі. Найбільш поширеним є Proof of Work (далі також – "PoW"), де валідація транзакцій здійснюється через розв'язання складних математичних задач, що потребує значних обчислювальних ресурсів [10]. Альтернативою виступає Proof of Stake (далі також – "PoS"), де право валідації визначається кількістю заблокованих токенів, що забезпечує більшу енергоефективність [28].

Механізми консенсусу в блокчейн-системах забезпечують узгодженість даних та безпеку мережі. PoW, перший історично впроваджений механізм, вимагає від валідаторів розв'язання складних криптографічних задач. Процес передбачає підбір спеціального значення. Складність підбору постійно коригується мережею для забезпечення стабільного часу створення блоків [11].

PoS суттєво відрізняється підходом до валідації. Валідатори блокують певну кількість токенів як заставу, а їхня вага при голосуванні пропорційна розміру стейку. Система використовує псевдовипадковий вибір валідаторів для кожного блоку, враховуючи їхню частку в загальному стейку. При виявленні шахрайських дій валідатор втрачає токени, що створює економічну мотивацію для чесної поведінки [28, 29].

Delegated Proof of Stake (далі також – "DPoS") представляє гібридний підхід, де власники токенів делегують право валідації обмеженій кількості нодів. Система працює як представницька демократія, де валідатори обираються голосуванням, а

їхня ефективність постійно оцінюється спільнотою. Це дозволяє досягти вищої пропускної здатності, але створює певну централізацію [30].

Порівняльний аналіз ефективності різних механізмів консенсусу демонструє суттєві відмінності. За даними дослідження Ethereum Foundation, PoS знижує енергоспоживання на 99.95% порівняно з PoW. При цьому швидкість підтвердження транзакцій у PoS-системах в середньому в 5-7 разів вища. DPoS показує найвищу пропускну здатність – до 4000 транзакцій в секунду, проте має нижчий рівень децентралізації. Практика впровадження різних механізмів консенсусу в публічних та приватних блокчейнах демонструє необхідність балансу між продуктивністю, безпекою та рівнем децентралізації [31].

Технічні характеристики блокчейну безпосередньо визначають правові наслідки. Незмінність даних, яка досягається через криптографічне зв'язування блоків, має наслідком високу доказову силу записів та неможливість підробки історії транзакцій [3].

Децентралізація, що реалізується через розподілене зберігання та валідацію, призводить до відсутності єдиного центру відповідальності та появи нових механізмів досягнення консенсусу [10, 16].

Автоматичне виконання, яке забезпечується смарт-контрактами та програмним кодом, трансформує традиційні механізми забезпечення виконання зобов'язань [5].

Прозорість, що досягається через публічний доступ до історії транзакцій, встановлює нові стандарти розкриття інформації та аудиту [1, 2].

Криптографічна частина блокчейну реалізується через механізми хешування, асиметричну криптографію з використанням пар публічних та приватних ключів, а також цифрові підписи для підтвердження автентичності транзакцій [3]. Ці механізми забезпечують безпеку та незмінність даних у мережі.

Аналіз технічних показників основних блокчейн-мереж демонструє суттєвий прогрес. З погляду продуктивності, Bitcoin обробляє в середньому 300,000 транзакцій щодня, час підтвердження транзакцій варіюється від 10 хвилин у Bitcoin до кількох секунд у нових блокчейнах мереж Layer 1 (далі також – "L1"), а пропускна здатність мереж Layer 2 (далі також – "L2") досягає понад 4,000 транзакцій в секунду [32].

Показники децентралізації та безпеки також вражають: кількість активних валідаторів у мережі Ethereum перевищила 900,000 після переходу на PoS, а енергоспоживання мережі знизилось на 99.9% [33].

Щодо масштабування, розмір блокчейну Bitcoin перевищив 500 гігабайт, кількість смарт-контрактів в Ethereum досягла понад 2 мільйонів, а середній розмір комісій знизився на 90% завдяки рішенням L2 [34].

Масштабованість залишається проблемним аспектом блокчейн-систем, що стимулює розвиток L2-рішень та оптимізацію протоколів консенсусу [35].

Розуміння технічних аспектів має важливе значення для правового регулювання, оскільки вони визначають можливості та обмеження при реалізації прав учасників блокчейн-відносин, а також впливають на формування механізмів захисту [21].

Аналіз технічних ризиків блокчейн-систем виявляє кілька критичних аспектів:

- Атака 51% залишається актуальною загрозою для малих блокчейн-мереж.
- Вразливості смарт-контрактів призвели до втрат понад 3.8 мільярдів доларів у 2022 році.
- Проблеми масштабованості обмежують широке впровадження технології [20, 36].

Для мінімізації цих ризиків розробляються технічні рішення:

- Впровадження механізмів крос-ланцюгової валідації.
- Удосконалення інструментів аудиту смарт-контрактів.
- Розвиток рішень L2 для підвищення масштабованості [37].

Інформаційні процеси в блокчейні мають унікальні характеристики, що відрізняють їх від традиційних систем обробки даних. Особливістю є розподілений характер зберігання інформації, при якому кожен вузол містить повну копію реєстру транзакцій, що забезпечує стійкість системи до збоїв та спроб маніпуляції.

Процес передачі інформації в блокчейні реалізується через механізм транзакцій, які групуються в блоки та підтверджуються учасниками мережі. Кожен новий блок містить криптографічний хеш попереднього блоку, створюючи нерозривний ланцюг

записів. Така архітектура забезпечує незмінність історії транзакцій та можливість верифікації будь-якої операції з моменту створення мережі [10, 11].

Безпека даних у блокчейні забезпечується комбінацією криптографічних методів та економічних стимулів. Використання цифрових підписів гарантує, що тільки власник приватного ключа може ініціювати транзакції, а механізми консенсусу запобігають подвійним витратам та іншим формам маніпуляцій [3].

Особливої уваги заслуговує питання конфіденційності в блокчейн-мережах. Хоча всі транзакції є публічними та прозорими, використання криптографічних адрес забезпечує певний рівень псевдонімності. Водночас розвиток методів аналізу даних створює виклики для збереження приватності користувачів, що вимагає впровадження додаткових механізмів захисту персональних даних [26].

Розуміння специфіки інформаційних процесів у блокчейні має принципове значення для формування адекватних правових механізмів регулювання та захисту прав. Особливості блокчейну створюють як нові можливості для забезпечення прозорості та довіри, так і специфічні виклики для традиційних правових інститутів [1, 16].

Розвиток блокчейн-технологій призвів до формування різних типів мереж, що відрізняються за механізмами доступу, управління та валідації транзакцій. Розуміння особливостей кожного типу має важливе значення для правового регулювання відносин, що виникають при їх використанні [15].

Публічні блокчейни характеризуються відкритістю та децентралізацією. Будь-який учасник може приєднатися до мережі, переглядати історію та брати участь у валідації. Bitcoin та Ethereum є прикладами таких систем, де прозорість та відсутність централізованого контролю є фундаментальними принципами функціонування [11, 27].

Правове регулювання різних типів блокчейн-систем вимагає врахування специфіки кожного з них, зокрема в контексті дотримання вимог GDPR щодо захисту персональних даних [38].

Приватні блокчейни, на відміну від публічних, функціонують як закриті системи з обмеженим доступом. Право участі в мережі та валідації транзакцій надається лише

авторизованим учасникам. Такі системи часто використовуються корпораціями та фінансовими установами для оптимізації внутрішніх процесів, забезпечуючи вищу продуктивність та контрольованість операцій [39].

Консорціумні блокчейни представляють гібридний підхід, де управління мережею здійснюється групою організацій. Цей тип особливо актуальний для міжгалузевої співпраці, наприклад, у логістичних ланцюгах або банківських консорціумах. Процес валідації здійснюється заздалегідь визначеними вузлами, що забезпечує баланс між децентралізацією та контролем [37].

Кожен тип блокчейн-систем має свої правові особливості та виклики. Публічні блокчейни стикаються з питаннями регулювання криптовалют та захисту прав користувачів. Приватні та консорціумні системи вимагають чіткого визначення відповідальності операторів та механізмів вирішення спорів між учасниками [40].

Відповідно до статті 1 Закону України "Про інформацію", інформаційні відносини охоплюють процеси створення, отримання, зберігання, поширення та використання інформації у фізичній чи електронній формах [8]. Технічні особливості блокчейну створюють новий контекст для реалізації цих процесів, вимагаючи переосмислення традиційних правових підходів.

Юридичне значення технічних особливостей блокчейну проявляється насамперед у незмінності та простежуваності інформації. Криптографічні механізми та розподілене зберігання даних створюють надійну систему доказів здійснення транзакцій та встановлення їх хронології. Це має особливе значення для вирішення спорів та підтвердження прав власності на цифрові активи [3].

Технічні обмеження блокчейну, такі як неможливість видалення чи модифікації даних, створюють специфічні правові виклики. Зокрема, виникають питання щодо реалізації права на забуття, виконання судових рішень про видалення інформації, а також виправлення помилок у смарт-контрактах [24].

Питання відповідальності за технічні збої та помилки в блокчейн-системах потребує особливої уваги. Децентралізований характер мережі ускладнює визначення відповідальної сторони, особливо у випадках, коли збій виникає через особливості протоколу консенсусу або помилки в коді смарт-контракту [36].

Порівняльний аналіз технічної імплементації блокчейну в різних правових системах виявляє:

- Різні підходи до вибору механізмів консенсусу (PoW vs PoS).
- Відмінності в технічних вимогах до учасників мережі.
- Специфіку технічних стандартів та протоколів [16].

Технічні особливості блокчейну створюють специфічний контекст для правового регулювання. Зокрема, незмінність даних, криптографічні механізми захисту та децентралізований характер обробки інформації вимагають нових підходів до забезпечення прав учасників та вирішення правових конфліктів [1].

Аналіз судової практики демонструє основні виклики, пов'язані з технічними особливостями блокчейну:

- Складність встановлення юрисдикції через розподілений характер мережі [41].
- Проблеми ідентифікації власників криптоактивів [42].
- Питання доказування прав на криптоактиви при банкрутстві криптобірж [43].

Технічні обмеження блокчейн-технології створюють специфічні виклики для правового регулювання:

Як було детально проаналізовано в Розділі 1.1, технічні обмеження блокчейн-технології створюють специфічні виклики для правового регулювання. Ці технічні обмеження вимагають розробки відповідних правових механізмів, зокрема:

1. Для подолання проблеми масштабованості - створення правової бази для L2-рішень та міжмережевих протоколів, з чітким визначенням відповідальності різних рівнів мережі.
2. Щодо енергоспоживання - впровадження екологічних стандартів та стимулювання переходу до енергоефективних механізмів консенсусу через податкові пільги та субсидії [28].

3. Для вирішення проблеми незворотності транзакцій - розробка правових механізмів компенсації та страхування ризиків, пов'язаних з помилковими операціями.
4. Для регулювання міждержавного характеру блокчейну - розвиток міжнародної гармонізації та координації регуляторних підходів [26].

Технічні обмеження блокчейну мають фундаментальний характер і впливають на можливості його практичного застосування. Проблема масштабованості проявляється у зниженні швидкості обробки транзакцій при зростанні навантаження на мережу. У Bitcoin це призводить до збільшення часу підтвердження транзакцій з кількох хвилин до кількох годин у періоди пікового навантаження. Ethereum стикається з подібними обмеженнями, що призводить до зростання вартості газу та ускладнює використання децентралізованих додатків (далі також – "DApps") [11].

Обмеження розміру блоку створює компроміс між пропускною здатністю та децентралізацією. Збільшення розміру блоку покращує швидкість обробки транзакцій, але підвищує вимоги до обчислювальних ресурсів вузлів, що може призвести до зменшення кількості учасників мережі. Це особливо критично для публічних блокчейнів, де важлива широка участь користувачів [10].

Проблема зберігання даних стає все гострішою з ростом блокчейн-мереж. Повні вузли повинні зберігати всю історію транзакцій, що призводить до постійного збільшення вимог до дискового простору [44].

Обмеження між різними блокчейнами створює фрагментацію екосистеми. Відсутність стандартизованих протоколів взаємодії ускладнює передачу активів між мережами [45].

Ці обмеження враховуються при формуванні регуляторних підходів у різних країнах, що буде детально розглянуто в Розділі 3.

Розвиток блокчейн-технологій супроводжується появою специфічних ризиків та загроз, що потребують особливої уваги при формуванні правового регулювання. Технологічні ризики насамперед пов'язані з вразливостями програмного коду та можливостями його експлуатації зловмисниками. Критичні помилки в смарт-

контрактах призводять до значних фінансових втрат, як показав випадок з The DAO, де через вразливість коду було втрачено близько 150 мільйонів доларів [46].

Безпекові загрози проявляються у можливості проведення атак на блокчейн-мережі. Атака 51% залишається актуальною для малих мереж, де зловмисник може отримати контроль над більшістю обчислювальної потужності. Атаки на криптовалютні біржі та гаманці користувачів призводять до втрати коштів через компрометацію приватних ключів або вразливості в інфраструктурі зберігання [20].

Операційні ризики включають можливість втрати доступу до активів через втрату приватних ключів, помилки при здійсненні транзакцій через незворотність операцій, а також ризики, пов'язані з людським фактором при взаємодії з блокчейн-системами. Статистика показує, що значна частина втрат у блокчейн-середовищі пов'язана саме з операційними помилками користувачів [14].

Регуляторні ризики виникають через невизначеність правового статусу блокчейн-активів та операцій з ними в різних юрисдикціях. Зміни в регулюванні можуть суттєво впливати на функціонування блокчейн-проєктів та вартість криптоактивів. Особливої гостроти набувають питання відповідності операцій вимогам AML та фінансуванню тероризму (далі також – "CFT") [47].

Репутаційні ризики пов'язані з використанням блокчейн-технологій для нелегальної діяльності, що створює негативне сприйняття технології суспільством та регуляторами. Випадки шахрайства з первинною пропозицією монет (далі також – "ICO") та криптовалютними проєктами підривають довіру до галузі та ускладнюють впровадження блокчейн-рішень [48].

Системні ризики проявляються у взаємозв'язку різних компонентів блокчейн-екосистеми. Проблеми одного великого проєкту можуть спричинити ланцюгову реакцію та вплинути на стабільність інших проєктів, як показав колапс криптобіржі FTX та його вплив на криптовалютний ринок [49].

Екологічні ризики пов'язані з високим енергоспоживанням мереж, що використовують механізм PoW. Це створює не лише екологічні, але й ризики для сталого розвитку технології через можливі регуляторні обмеження [29].

Формування ефективної системи управління ризиками у блокчейн-середовищі потребує комплексного підходу, що включає технічні рішення, правові механізми та освітні ініціативи для підвищення обізнаності користувачів. Розвиток стандартів безпеки, впровадження механізмів аудиту смарт-контрактів та створення систем страхування ризиків стають важливими елементами зрілої блокчейн-екосистеми [2, 16].

Дослідження технічних аспектів функціонування блокчейну та їх правових імплікацій формує методологічну основу для аналізу міжнародного досвіду регулювання в Розділі 3. Виявлені технічні обмеження та особливості мають вплив на формування регуляторних підходів у різних юрисдикціях та визначають специфіку правового регулювання блокчейн-технологій на міжнародному рівні [50].

Технічні особливості блокчейну безпосередньо впливають на правовий статус та функції різних категорій учасників блокчейн-відносин. Розуміння цього взаємозв'язку є ключовим для аналізу суб'єктного складу таких відносин.

1.2. Суб'єкти та об'єкти блокчейн-відносин

Технічні особливості блокчейну формують специфічне середовище для взаємодії різних категорій суб'єктів, аналіз яких необхідний для розуміння механізмів правового регулювання.

У рамках інформаційного права суб'єктами правовідносин вважаються особи, що беруть участь у створенні, обробці та передачі інформації [22]. Проте у контексті блокчейн-технології це визначення потребує суттєвого розширення, оскільки взаємодія в децентралізованому середовищі має свою специфіку.

Суб'єкт блокчейн-відносин — це учасник децентралізованої мережі, який має технічну можливість та правові підстави для участі в створенні, передачі, зберіганні та обробці інформації в блокчейні. Такими суб'єктами можуть бути як фізичні та юридичні особи, так і державні органи, що взаємодіють з блокчейн-мережею.

Порівняльно-правовий аналіз статусу суб'єктів блокчейн-відносин показує:

- Різний правовий статус криптовалютних бірж (від повноцінних фінансових установ до нерегульованих платформ).
- Відмінності у вимогах до майнерів та валідаторів.
- Специфіку регулювання діяльності розробників та організаторів ICO [51].

Критерії класифікації суб'єктів блокчейн-відносин:

1. Роль: творці та валідатори; користувачі; посередники; регулятори;
2. Правовий статус: фізичні та юридичні особи; держави; міжнародні організації;
3. Мета участі: комерційні; некомерційні; регуляторні.

Статистика користування блокчейн-сервісами показує:

- 52% інституційних інвесторів вже інвестують у криптоактиви.
- 76% великих банків планують впровадити блокчейн-рішення до 2025 року.
- Кількість зареєстрованих користувачів криптобірж перевищила 300 мільйонів.
- 25% малих підприємств планують прийняти криптоплатежі у 2024 році [52].

Звичайними користувачами вважаються особи, що застосовують блокчейн для зберігання чи переказу криптовалют, участі в DApps чи інших сервісах [39]. Користувачі є найчисельнішою групою суб'єктів таких відносин. За метою їх участі в блокчейн-мережах можна виділити такі категорії:

1. За типом активності: інвестори (купують та утримують криптоактиви з метою отримання прибутку), трейдери (здійснюють активну торгівлю на криптовалютних біржах) та звичайні користувачі (здійснюють платежі чи користуються децентралізованими сервісами).
2. За характером участі: активні (регулярно здійснюють операції в мережі) та пасивні (переважно зберігають активи без частих транзакцій).
3. За рівнем технічної підготовки: професійні (мають розуміння технології) та початківці (потребують спрощених інтерфейсів та додаткового захисту).

Статистичні дані демонструють зростання кількості користувачів блокчейн-систем. За даними Chainalysis, у 2023 році кількість активних криптогаманців перевищила 420 мільйонів, з яких близько 30% припадає на регулярних користувачів. Аналіз показує, що 60% користувачів використовують криптовалюти для інвестицій, 25% - для платежів, і 15% - для доступу до децентралізованих сервісів. При цьому рівень технічної грамотності користувачів залишається критичним фактором: 70% випадків втрати коштів пов'язані з людським фактором [53].

Правовий статус користувачів визначається законодавством конкретної юрисдикції, умовами використання платформ та типом здійснюваних операцій. Основними правами є доступ до мережі, здійснення транзакцій, використання смарт-контрактів та захист персональних даних. До обов'язків належать дотримання правил мережі, забезпечення безпеки ключів та виконання вимог законодавства.

Таким чином, користувачі як найчисельніша група суб'єктів блокчейн-відносин мають чітко визначені права та обов'язки, але їх правовий статус значною мірою залежить від юрисдикції та типу використовуваних блокчейн-сервісів, що створює необхідність особливої уваги до захисту їхніх прав та інтересів.

Компанії та підприємці можуть інтегрувати блокчейн у свої процеси, прагнучи прозорості, зменшення витрат і відмови від посередників [32]. Підприємницькі суб'єкти в блокчейн-середовищі можна класифікувати за кількома критеріями.

Підприємства в блокчейн-середовищі різняться за масштабом. Великі корпорації мають ресурси для повної інтеграції блокчейну, середні підприємства впроваджують окремі рішення, а малі підприємства зазвичай користуються готовими сервісами.

За сферою діяльності виділяються технологічні компанії, які розробляють блокчейн-рішення; торгові підприємства, що використовують технологію для оптимізації; виробничі компанії, які застосовують блокчейн для контролю ланцюгів постачання; та сервісні компанії, що впроваджують блокчейн для автоматизації.

Особливості використання блокчейну в бізнес-процесах проявляються через автоматизацію розрахунків, токенізацію активів та управління ланцюгами постачання. Це дозволяє оптимізувати взаємодію з клієнтами та партнерами [54].

Правове регулювання такої діяльності вимагає дотримання вимог різних юрисдикцій, забезпечення захисту комерційної таємниці в умовах прозорого середовища, а також розв'язання питань відповідальності за помилки в смарт-контрактах та механізмів врегулювання транскордонних спорів.

Отже, підприємства як суб'єкти блокчейн-відносин стикаються з подвійним викликом: з одного боку, необхідністю впровадження інноваційних технологічних рішень, а з іншого — забезпеченням відповідності різноманітним регуляторним вимогам та захистом своїх комерційних інтересів у децентралізованому середовищі.

Фінансові установи мають особливий статус через їхню діяльність та наявність регуляторних вимог. Можна виділити види фінансових установ за типом діяльності:

1. Криптовалютні біржі — забезпечують торгівлю та обмін криптоактивів;
2. Платіжні системи — здійснюють перекази та розрахунки криптоактивів;
3. Інвестиційні фонди — управляють та інвестують криптоактиви;
4. Традиційні банки — впроваджують блокчейн-рішення в класичні операції [55].

Фінансові установи в блокчейн-середовищі виступають особливими суб'єктами інформаційних відносин, що забезпечують створення, обробку та передачу даних про цифрові активи. Їх діяльність характеризується специфічними інформаційними процесами: валідацією транзакцій, веденням розподілених реєстрів операцій, забезпеченням цілісності та достовірності даних про цифрові активи.

Правовий статус таких установ характеризується підвищеною відповідальністю перед клієнтами, необхідністю дотримання банківської таємниці та регулярної звітності перед наглядовими органами. Важливими аспектами є також страхування ризиків та дотримання особливих вимог до корпоративного управління [18, 22].

Таким чином, фінансові установи в блокчейн-середовищі поєднують традиційні фінансові функції з інноваційними технологічними рішеннями, що вимагає особливого підходу до їх регулювання та нагляду.

Майнери підтримують стабільність мереж, побудованих за алгоритмом PoW (Bitcoin, Ethereum до переходу на PoS), розв’язуючи криптографічні задачі. За успішний видобуток блоку вони отримують нові монети й комісію [11]. У деяких

країнах майнінг може підлягати ліцензуванню чи оподаткуванню, в інших — заборонятися через енергоспоживання.

З’являються також майнери PoS (валідатори), однак їхня специфіка ("ставка" монет замість обчислювальних задач) має свої особливості.

Майнери та валідатори відіграють ключову роль у функціонуванні блокчейн-мереж, але мають різні механізми роботи. Майнери забезпечують перевірку транзакцій, створюють блоки та отримують винагороду за підтримку мережі. Їхня діяльність характеризується високою енергозатратністю, потребою в спеціальному обладнанні та конкуренцією за обчислювальну потужність.

Валідатори, які працюють у системах PoS, підтверджують транзакції через механізм стейкінгу. Вони вносять заставу замість витрат на обчислення, можуть втратити її за недобросовісну поведінку та повинні забезпечувати підключення до мережі. Їх статус більш наближений до фінансових посередників [28, 31].

Спільними аспектами правового статусу майнерів та валідаторів є необхідність визначення характеру їхньої діяльності як підприємницької, особливості оподаткування та відповідальність за забезпечення стабільності мережі.

Держави все частіше інтегрують блокчейн в управління з метою прозорості та зменшення корупційних ризиків. Технологія знаходить застосування в різних сферах державного управління: для організації електронного голосування зі зберіганням бюлетенів у реєстрі, створення реєстрів власності на нерухомість, забезпечення цифрових документів, таких як паспорти чи посвідчення водія, та автоматизації соціальних виплат через смарт-контракти [57].

Головним викликом є правове обґрунтування ролі держави у децентралізованій мережі та узгодження з принципами законодавства про державні послуги.

Державні органи та регулятори виконують подвійну роль у блокчейн-середовищі. Як користувачі технології, вони впроваджують державні реєстри на блокчейні, використовують його для електронного голосування, автоматизують державні послуги та здійснюють управління державними активами.

У ролі регуляторів вони встановлюють правила діяльності на криптовалютному ринку, здійснюють ліцензування учасників, контролюють дотримання законодавства та забезпечують захист прав споживачів [19, 58].

Регуляторні функції державних органів охоплюють класифікацію криптоактивів, формування вимог до діяльності бірж, здійснення нагляду за проведенням ICO/IEO та забезпечення протидії відмиванню коштів. Важливим аспектом є також координація регуляторних підходів між різними державними інституціями [47].

Функції регуляторів включать ліцензування та нагляд за криптовалютними біржами, контроль за дотриманням AML/KYC вимог, захист прав споживачів послуг, моніторинг системних ризиків та координація з міжнародними регуляторами.

Інструменти регулювання насамперед це розробка спеціального законодавства, впровадження "регуляторних пісочниць", створення систем звітності та моніторингу та розвиток механізмів оперативного реагування на ризики.

Викликами для регуляторів є балансування між інноваціями та безпекою, адаптація наглядових практик до децентралізованого середовища, розвиток технічних компетенцій та міжнародна координація регуляторних дій.

Цей аналіз створює основу для розгляду перспектив розвитку регулювання в Україні, що буде детально висвітлено в Розділі 4.

Розробники створюють DApps і відповідають за програмний код (чому можуть виникати запитання про відповідальність у разі вразливостей) [59].

Категорії розробників блокчейн-рішень: розробники протоколів, які створюють і підтримують інфраструктуру блокчейну; розробники DApps, які створюють додатки на наявних блокчейн-платформах; розробники смарт-контрактів, які створюють код для автоматизації транзакцій та розробники інфраструктури, які створюють інструменти взаємодії в блокчейні.

Правовий статус розробників: відповідальність за якість та безпеку; гарантійні зобов'язання; права на інтелектуальну власність; механізми оновлення та підтримки програмного забезпечення; відповідальність за помилки та вразливості [36, 40].

Організатори ICO/IEO випускають токени, залучаючи криптовалюту від інвесторів. Якщо токени підпадають під визначення "цінних паперів", до організаторів можуть застосовуватися закони про емісію [60].

Структура ICO/IEO визначається обраною юрисдикцією, організаційною формою та корпоративною структурою проєкту. При цьому організатори зобов'язані забезпечити повне розкриття інформації через White Paper, технічну документацію, фінансову звітність та дорожню карту проєкту [48, 51].

Регуляторні вимоги до проєктів ICO/IEO включають відповідність законодавству про цінні папери, необхідність ліцензування діяльності та забезпечення прозорості для захисту прав інвесторів.

Відповідальність розробників та організаторів ICO/IEO має подвійний характер: технічний аспект охоплює якість, безпеку та своєчасне оновлення програмного забезпечення, тоді як юридичний стосується відповідальності перед користувачами, інвесторами та регуляторними органами.

Отже, розробники та організатори ICO/IEO є суб'єктами в розвитку блокчейн-екосистеми, що несуть відповідальність за технічну та юридичну частину проєктів.

Серед користувачів існує думка, що смарт-контракти можуть розглядатися як суб’єкти завдяки автономній дії. Проте традиційне право визнає суб’єктами лише фізичних і юридичних осіб, наділених правоздатністю [61]. Смарт-контракт — це програмний код, що автоматично виконує умови, проте не має "свідомості" чи "волі".

Надалі, з розвитком штучного інтелекту, дискусія може загостритися, але наразі смарт-контракт не вважається суб’єктом. Він діє "від імені" сторін договору.

Питання правосуб'єктності в блокчейн-середовищі набуває особливої складності через специфіку децентралізованих взаємодій. Традиційне розуміння правосуб'єктності, що базується на волевиявленні та дієздатності, трансформується в контексті автоматизованих систем та смарт-контрактів [5, 62].

Особливої уваги заслуговує питання правосуб'єктності децентралізованих автономних організацій (далі також – "DAO", не плутати з "The DAO – це конкретна назва організації). Такі організації функціонують на основі смарт-контрактів та не мають традиційної корпоративної структури, що створює виклики для визначення їх

правового статусу. У деяких юрисдикціях вже з'являються спеціальні форми юридичних осіб для DAO, що визнають їх обмежену правосуб'єктність [63].

Важливим аспектом є також питання делегованої правосуб'єктності в контексті використання смарт-контрактів та автоматизованих систем прийняття рішень. Хоча такі системи можуть автономно виконувати дії, їхня правосуб'єктність залишається похідною від правосуб'єктності учасників, які їх створили та використовують.

Розвиток технологій штучного інтелекту та їх інтеграція з блокчейном створює передумови для появи форм квазі-правосуб'єктності, де автоматизовані системи можуть мати обмежену автономію в прийнятті рішень та здійсненні юридично значущих дій. Це вимагає нових правових конструкцій та механізмів регулювання.

Правова природа смарт-контрактів визначається їх статусом як програмного коду, що виступає формою договору. Вони характеризуються автоматичним виконанням умов, незмінністю після активації та відсутністю правосуб'єктності [37].

Функціонування смарт-контрактів передбачає виконання дій від імені сторін та можливість взаємодії з іншими смарт-контрактами, хоча існують обмеження щодо модифікації та певні технічні ризики виконання.

Механізми взаємодії суб'єктів у блокчейн-середовищі можуть бути прямими, що включають peer-to-peer (далі також – "p2p") транзакції, смарт-контракти та децентралізовані платформи з автоматизованими протоколами, або здійснюватися через посередників, таких як криптовалютні біржі, платіжні системи, сервіси та професійні консультанти [23].

Вирішення спорів у блокчейн-середовищі забезпечується як технічними засобами (протоколи, мультипідписи, арбітражні смарт-контракти), так і правовими механізмами, що включають судовий захист, міжнародний арбітраж, медіацію та спеціалізовані блокчейн-трибунали [25, 64].

На основі вищенаведеного ми можемо встановити такі висновки та перспективи: необхідність розвитку збалансованої системи регулювання; важливість стандартизації процесів взаємодії; потреба в розвитку ефективних механізмів вирішення спорів; значення міжнародної координації та співпраці

Взаємодія суб'єктів у блокчейн-середовищі характеризується специфічними механізмами координації та комунікації, що базуються на технологічних протоколах та криптографічних методах. Це створює особливу систему інформаційних відносин, де технічні механізми стають основою правової взаємодії.

Таким чином, ефективне функціонування блокчейн-екосистеми вимагає комплексного підходу до вирішення технічних, правових та організаційних викликів, а також розвитку адекватних механізмів взаємодії між усіма суб'єктами.

Особливої уваги потребує розробка механізмів взаємодії між різними категоріями суб'єктів та забезпечення ефективного вирішення спорів між ними.

Аналіз суб'єктного складу блокчейн-відносин та специфіки їх взаємодії створює необхідну базу для розробки пропозицій щодо вдосконалення національного законодавства в Розділі 4. Розуміння ролей та інтересів різних категорій учасників, особливо регуляторів та фінансових установ, є критичним для формування ефективної моделі регулювання блокчейн-технологій в Україні [1, 2].

Взаємодія суб'єктів у блокчейн-середовищі нерозривно пов'язана з особливими об'єктами інформаційних відносин, які виникають у процесі такої взаємодії. Специфіка цих об'єктів потребує окремого детального аналізу.

Діяльність суб'єктів блокчейн-відносин спрямована на специфічні об'єкти, які потребують особливого правового режиму та захисту.

Інформаційні відносини у блокчейн-середовищі характеризуються специфічними об'єктами, що поєднують ознаки цифрових даних, фінансових інструментів та майнових прав. У широкому розумінні, об'єктом таких відносин виступає будь-яка інформація, що може бути зафіксована, збережена та передана за допомогою блокчейну [65]. Однак розвиток технології призвів до формування нових типів об'єктів, які вимагають особливого правового регулювання.

Класифікація об'єктів інформаційних відносин у блокчейн-середовищі має важливе теоретичне та практичне значення для їх регулювання. Вона дозволяє систематизувати цифрові об'єкти за їх правовою природою та функціональним призначенням, що сприяє формуванню чіткої регуляторної політики [21].

Основними ознаками об'єктів у блокчейн-середовищі є їх цифрова форма, використання криптографічних методів захисту, неможливість зміни даних без згоди учасників, розподілене зберігання та можливість відстеження історії змін [21].

За правовою природою об'єкти в блокчейні поділяються на:

1. Цифрові активи, що включають криптовалюти, токени та інші віртуальні активи, які можуть виконувати функції засобу обміну, накопичення чи інвестування.
2. Інформаційні об'єкти, такі як транзакційні дані, метадані та записи в розподіленому реєстрі.
3. Об'єкти інтелектуальної власності, включаючи програмний код, цифровий контент та токенізовані права на твори.

Розвиток цифрових активів створює потребу в новій правовій категоризації, яка враховувала б як технологічні особливості блокчейну, так і традиційні правові концепції. Зокрема, токени можуть одночасно проявляти властивості цінних паперів, товарів або засобів платежу, що ускладнює застосування існуючих регуляторних підходів [66].

Порівняльний аналіз регуляторних підходів до класифікації об'єктів у блокчейні демонструє суттєві відмінності між юрисдикціями. У США Комісія з цінних паперів і бірж (далі також – "SEC") застосовує тест Хауі (метод визначення чи є фінансовий інструмент інвестиційним контрактом) для визначення правового статусу токенів [66], тоді як ЄС у MiCA регламенті запроваджує комплексну систему класифікації криптоактивів, виділяючи платіжні токени, utility-токени та токени, забезпечені активами [67]. Японський підхід базується на функціональному призначенні активів, що дозволяє більш гнучко реагувати на появу нових форм цифрових активів [68].

Емпіричні дослідження ринку цифрових активів, проведені CoinGecko у 2024 році, демонструють домінування платіжних криптовалют, які складають майже половину ринкової капіталізації. Значну частку також займають інфраструктурні токени та активи DeFi, що свідчить про розвиток практичного застосування блокчейн-технологій у фінансовому секторі [69].

Міждисциплінарний аналіз впливу цифрових активів розкриває їх значний потенціал для трансформації фінансової системи. Економічні дослідження підтверджують зниження трансакційних витрат при використанні блокчейн-активів. Соціологічні спостереження вказують на зростання фінансової інклюзії, особливо серед раніше неохоплених банківськими послугами груп населення. Технологічний аспект проявляється у підвищенні прозорості та простежуваності операцій.

Особливістю правового режиму цих об'єктів є їх подвійна природа. З одного боку, вони є інформаційними об'єктами, що підпадають під дію законодавства про інформацію [8], а з іншого — можуть мати майнову цінність та бути предметом цивільного обороту.

Специфіка блокчейну створює особливі умови для функціонування об'єктів: незворотність транзакцій, неможливість примусового вилучення, складність ідентифікації власників та транскордонний характер обігу. Це вимагає розробки спеціальних правових механізмів регулювання, які враховували б як технологічні особливості блокчейну, так і необхідність захисту прав учасників [37].

Смарт-контракти є особливим видом програмних об'єктів в інформаційних відносинах, що характеризуються здатністю автономно обробляти та передавати інформацію в блокчейн-мережі. З погляду інформаційного права, смарт-контракти становлять собою цифрові протоколи, які забезпечують автоматизовану обробку даних за визначеними алгоритмами [36].

За функціональним призначенням смарт-контракти поділяються на кілька основних груп. Фінансові смарт-контракти включають платіжні, що забезпечують автоматизацію розрахунків та переказів; кредитні, які реалізують механізми позик та забезпечення; інвестиційні, що відповідають за токенізацію активів та управління портфелями; а також DeFi-контракти, що забезпечують роботу протоколів DeFi.

Управлінські смарт-контракти охоплюють контракти корпоративного управління для голосування та розподілу дивідендів, контракти управління доступом для контролю прав та повноважень, реєстраційні для ведення обліку, та адміністративні для автоматизації бізнес-процесів [36].

Сервісні смарт-контракти представлені ігровими контрактами для реалізації ігрової механіки, ідентифікаційними для управління цифровими ідентичностями, логістичними для відстеження поставок та документообігу, а також ліцензійними для управління правами інтелектуальної власності.

За рівнем складності смарт-контракти розділяються на прості, що виконують базові операції передачі активів; складені, що поєднують кілька функцій; та комплексні, що реалізують складну бізнес-логіку з множинними умовами.

Інформаційна природа смарт-контрактів проявляється через їх основні характеристики як об'єктів інформаційних відносин:

- програмний код як форма фіксації інформації про умови та алгоритми обробки даних
- криптографічний захист інформації, що обробляється
- незмінність записаної інформації після розміщення в блокчейні
- прозорість процесів обробки інформації для всіх учасників мережі [5]

Особливістю смарт-контрактів як інформаційних об'єктів є їх здатність взаємодіяти з різними джерелами даних. Через систему оракулів вони можуть отримувати інформацію з зовнішніх джерел, обробляти її та генерувати нові інформаційні записи в блокчейні. При цьому кожна така операція є простежуваною та верифікованою.

Технічна реалізація смарт-контрактів включає:

- унікальний ідентифікатор (адресу) в блокчейн-мережі
- набір функцій для обробки інформації
- механізми взаємодії з іншими смарт-контрактами
- протоколи валідації та верифікації інформації [5]

В інформаційно-правовому аспекті важливим є питання достовірності та цілісності даних, що обробляються смарт-контрактами. Незмінність коду після розміщення в блокчейні забезпечує стабільність алгоритмів обробки інформації, але одночасно створює виклики при виявленні помилок у логіці обробки даних.

Розвиток смарт-контрактів як інформаційних об'єктів відбувається в напрямку вдосконалення механізмів обробки та захисту інформації. Особливої уваги заслуговують питання:

- стандартизації форматів даних
- розвитку протоколів міжмережевої взаємодії
- вдосконалення механізмів верифікації інформації
- забезпечення конфіденційності при обробці персональних даних [26]

З позиції інформаційної безпеки, смарт-контракти створюють нові виклики щодо захисту інформації. Публічність коду дозволяє проводити аудит механізмів обробки даних, але також робить вразливості видимими для потенційних атак [20]. Це вимагає розвитку спеціальних методів тестування та валідації програмного коду.

Таким чином, смарт-контракти як об'єкти інформаційних відносин являють собою складні програмні комплекси, що забезпечують автоматизовану обробку інформації в блокчейн-середовищі. Їх подальший розвиток вимагає вдосконалення механізмів захисту інформації та стандартизації процесів обробки даних.

Цифрові (віртуальні) активи представляють особливий вид інформаційних об'єктів у блокчейн-середовищі, що характеризуються специфічним способом створення, зберігання та передачі даних. Їх унікальність полягає в тому, що вони поєднують властивості інформаційного ресурсу з можливістю представлення цінності в цифровій формі [66].

Важливо розмежувати поняття "криптовалюта" та "віртуальний актив". Віртуальний актив є ширшим поняттям, що охоплює будь-які цінності, які існують у цифровій формі та функціонують за допомогою технології розподіленого реєстру. Криптовалюта є одним із видів віртуальних активів, що характеризується наступними особливостями: використовується переважно як засіб платежу або обміну; має власну одиницю обліку; не має централізованого емітента та функціонує на основі криптографічних методів [11].

Таким чином, всі криптовалюти є віртуальними активами, але не всі віртуальні активи є криптовалютами. До віртуальних активів також належать:

- - Utility-токени, що надають доступ до певних сервісів.
- - Security-токени, що представляють права на традиційні фінансові активи.
- - NFT, що засвідчують право на унікальні цифрові об'єкти.
- - Стейблкоїни, що прив'язані до вартості фіатних валют або інших активів.

Цифрові активи можна класифікувати за різними критеріями, що відображають їх багатогранну природу.

Залежно від забезпеченості розрізняють незабезпечені активи, такі як Bitcoin та Ethereum, забезпечені фіатними валютами, як USDT та USDC, забезпечені товарними активами, наприклад, золотом чи нерухомістю, та забезпечені іншими криптоактивами.

Сфера застосування визначає поділ на універсальні активи загального призначення, галузеві для конкретних індустрій, проєктні для окремих проєктів та корпоративні для внутрішнього використання. Технічна реалізація включає нативні токени блокчейн-платформ, токени різних стандартів тощо [47].

В інформаційно-правовому аспекті цифрові активи характеризуються криптографічним кодуванням інформації про право доступу та розпорядження активом, розподіленим характером зберігання даних, алгоритмічною верифікацією історії транзакцій та можливістю програмного управління через смарт-контракти.

Структура інформації про цифровий актив є комплексною та включає метадані про створення та емісію, історію всіх транзакцій, криптографічні докази володіння та технічні параметри функціонування. Ця інформація зберігається в розподіленому реєстрі та доступна для верифікації всіма учасниками мережі [3].

З погляду обробки інформації, цифрові активи можуть існувати як нативні токени мереж, токенізовані активи, що представляють інформацію про реальні об'єкти, та інформаційні токени, що надають доступ до даних чи сервісів.

Інформаційна природа цифрових активів проявляється через їх існування виключно у формі записів у розподіленому реєстрі. На відміну від традиційних

об'єктів обліку, інформація про цифрові активи не може бути змінена чи видалена, а її достовірність забезпечується математичними алгоритмами та колективною верифікацією. Це створює новий тип інформаційних об'єктів, де технічні механізми захисту є невіддільною частиною їх сутності.

Особливістю інформаційних процесів при роботі з цифровими активами є їх повна простежуваність та незворотність. Кожна операція з активом залишає незмінний інформаційний слід у блокчейні, що створює повну історію всіх транзакцій. Це формує новий стандарт прозорості інформаційних відносин.

Захист інформації про цифрові активи забезпечується через криптографічні механізми контролю доступу, розподілене зберігання даних та консенсусні протоколи валідації інформації. На відміну від традиційних баз даних, де інформація централізовано контролюється адміністратором, у блокчейні захист реалізується через технічні протоколи та математичні алгоритми [10].

У контексті обробки персональних даних, пов'язаних з цифровими активами, виникають специфічні виклики. Публічність блокчейну створює необхідність розробки спеціальних механізмів забезпечення конфіденційності при збереженні можливості верифікації транзакцій [26].

Розвиток інформаційних технологій призводить до появи нових форм цифрових активів, що вимагає постійного вдосконалення механізмів обробки та захисту інформації. Особливої уваги потребують питання стандартизації форматів даних, розвитку протоколів міжмережевої взаємодії та забезпечення сумісності різних інформаційних систем [50].

Таким чином, цифрові активи як об'єкти інформаційних відносин характеризуються унікальним поєднанням властивостей інформаційного ресурсу та цифрового представлення цінності. Їх подальший розвиток вимагає вдосконалення механізмів обробки та захисту інформації, стандартизації процесів та забезпечення балансу між прозорістю та конфіденційністю.

NFT є особливим видом цифрових активів, що характеризується унікальністю та неможливістю взаємозаміни. На відміну від криптовалют, де кожна одиниця ідентична, кожен NFT має унікальні характеристики та властивості, що відкриває нові

можливості для цифрового підтвердження права власності та автентичності [70, 71, 72].

Технічні характеристики NFT включають унікальний ідентифікатор у блокчейні, неподільність токену, незмінність метаданих та можливість підтвердження походження. Функціонально вони забезпечують цифрове підтвердження права власності, засвідчення автентичності та можливість передачі прав [73].

Правова природа NFT характеризується дуальністю: технічно це запис у реєстрі з унікальним ідентифікатором, а юридично – цифровий актив, що засвідчує певні права щодо об'єкта токенізації. Ключовим аспектом регулювання є розмежування прав на токен та на базовий актив, особливо для об'єктів інтелектуальної власності [73].

Специфіка NFT як об'єкта правовідносин проявляється також у способах передачі прав. Технологічна архітектура блокчейну забезпечує незмінність історії володіння та неможливість дублювання токену, що створює новий механізм підтвердження автентичності цифрових активів.

У контексті права власності та інтелектуальної власності NFT створюють складну правову конструкцію. Важливим є розмежування прав на сам токен та права на об'єкт, який він представляє. Володіння NFT не обов'язково означає володіння авторськими правами на твір, який токенізовано [74]. Це вимагає чіткого визначення обсягу прав, що передаються, та забезпечення захисту прав авторів.

Практичне застосування NFT охоплює різні сфери:

1. Мистецтво та креативні індустрії (цифрові картини, музика, відео)
2. Ігрова індустрія (віртуальні предмети та землі)
3. Нерухомість (токенізація прав на нерухоме майно)
4. Освіта (цифрові дипломи та сертифікати)
5. Спорт та розваги (моменти матчів, цифрові квитки)

Правове регулювання NFT стикається з низкою викликів: визначення правового статусу, захист прав власників, оподаткування операцій, забезпечення технічної

надійності та зберігання метаданих. Особливої уваги потребує розвиток механізмів вирішення спорів та захисту прав споживачів.

Окрему категорію об'єктів інформаційних відносин у блокчейні становлять об'єкти спеціального призначення, використання яких регулюється особливими правовими режимами. Згідно з ЗУ "Про інформацію", такі об'єкти підпадають під особливі вимоги щодо створення, обробки та захисту інформації [8, 75].

Дані голосування в блокчейн-системах мають специфічний правовий режим, що поєднує вимоги виборчого законодавства з технологічними можливостями блокчейну. Ключовими характеристиками є незмінність записаних голосів, забезпечення анонімності виборців при одночасній можливості верифікації результатів [76, 77]. Особлива увага приділяється захисту таємниці голосування та відповідності процедур виборчому законодавству.

Реєстри та бази даних на блокчейні представляють особливий інтерес для державного управління. Їх характерними рисами є розподілене зберігання інформації, захист від несанкціонованої модифікації та можливість аудиту змін. Правовий статус таких реєстрів визначається спеціальним законодавством та вимагає чіткого регулювання порядку внесення змін та доступу до інформації [19].

Особливої уваги заслуговує питання обробки персональних даних у блокчейн-середовищі. Незмінність записів створює специфічні виклики щодо забезпечення права на забуття та відповідності вимогам GDPR. Необхідним є пошук балансу між прозорістю блокчейну та захистом конфіденційності при передачі даних [24, 26].

Державні інформаційні системи на базі блокчейну (цифрові посвідчення, майнові реєстри, податкові документи) вимагають особливого підходу до забезпечення безпеки та надійності. Їх функціонування повинно відповідати як технічним стандартам блокчейну, так і вимогам законодавства про захист інформації.

Інформаційні об'єкти спеціального призначення в блокчейні характеризуються особливим правовим режимом, що поєднує вимоги до захисту інформації з технологічними можливостями розподіленого реєстру. Це створює нову парадигму обробки та зберігання даних у державному секторі, де технологічні механізми забезпечують як достовірність інформації, так і її захист від втручання.

Перспективи розвитку спеціальних інформаційних об'єктів пов'язані з вдосконаленням механізмів захисту, розширенням сфер застосування та інтеграцією з державними системами. Особливого значення набуває розвиток міжнародних стандартів та гармонізація підходів до регулювання у різних юрисдикціях [50].

Об'єкти інформаційних відносин у блокчейн-середовищі представляють складну систему, що включає різні види цифрових активів та інформаційних об'єктів. У межах проведеного дослідження було систематизовано та проаналізовано основні категорії таких об'єктів.

Смарт-контракти визначено як базовий об'єкт блокчейн-відносин, що поєднує характеристики програмного коду та правового інструменту. Їх особливістю є автоматичне виконання умов та незмінність після розміщення в блокчейні, що створює нові можливості для автоматизації договірних відносин [5, 36].

Цифрові активи, включаючи криптовалюти та токени, формують особливу категорію об'єктів, що відрізняється від традиційних фінансових інструментів децентралізованим характером емісії та обігу. Їх правовий статус суттєво різниться залежно від юрисдикції, що створює виклики для міжнародного регулювання [67, 68].

NFT як специфічний вид цифрових активів відкривають нові можливості для підтвердження права власності на унікальні цифрові об'єкти. Водночас вони створюють складні правові конструкції, особливо в контексті взаємодії з правом інтелектуальної власності [72, 73].

Інформаційні об'єкти спеціального призначення, такі як дані голосування та державні реєстри, вимагають особливого правового режиму, що враховує як технологічні можливості блокчейну, так і вимоги спеціального законодавства.

Порівняльний аналіз правового режиму об'єктів у блокчейні виявляє:

- - Різні підходи до класифікації віртуальних активів.
- - Відмінності у визнанні правового статусу смарт-контрактів.
- - Специфіку регулювання NFT в різних юрисдикціях.

Загалом, дослідження показало необхідність розробки комплексного підходу до правового регулювання об'єктів у блокчейні, який би враховував їх технологічну специфіку та забезпечував ефективний захист прав учасників відносин.

Дослідження об'єктів інформаційних відносин у блокчейні та їх правового режиму безпосередньо пов'язане з аналізом приватно-правових механізмів у Розділі 2 та міжнародного досвіду в Розділі 3. Особливості правового статусу віртуальних активів, смарт-контрактів та NFT визначають специфіку їх регулювання як на національному, так і на міжнародному рівні.

Особливості правового режиму об'єктів у блокчейні визначають специфіку змісту інформаційних відносин, що виникають при їх використанні. Розглянемо детальніше юридичний та фактичний зміст цих відносин.

1.3. Зміст інформаційних відносин із застосуванням блокчейн-технології

Взаємодія суб'єктів щодо об'єктів у блокчейн-середовищі формує особливий зміст інформаційних відносин, який поєднує традиційні правові механізми з новими технологічними можливостями.

Зміст інформаційних відносин у блокчейн-середовищі являє складну систему взаємопов'язаних юридичних та фактичних елементів, що визначають сутність та особливості взаємодії учасників [37]. Специфіка цих відносин зумовлена унікальними характеристиками блокчейну та новими формами цифрової взаємодії.

Вплив блокчейну на базові принципи інформаційного права проявляється у декількох ключових аспектах. По-перше, змінюється розуміння доступності інформації — від дискреційної моделі доступу до повної прозорості для всіх учасників мережі. По-друге, трансформується принцип достовірності інформації, який забезпечується не авторитетом джерела, а математичними алгоритмами та колективною верифікацією. По-третє, принцип захисту інформації реалізується через технологічну архітектуру системи, а не через адміністративні механізми [78].

Під змістом інформаційних відносин у блокчейні розуміють сукупність суб'єктивних прав та юридичних обов'язків, фактичні дії щодо реалізації прав та обов'язків, а також процеси, що забезпечують функціонування відносин [76].

Юридичний зміст відносин охоплює систему суб'єктивних прав, серед яких право на володіння та розпорядження цифровими активами, право на здійснення транзакцій, право на участь у консенсусі та право на конфіденційність [23]. До юридичних обов'язків належать дотримання протоколів мережі, виконання умов смарт-контрактів, дотримання вимог та забезпечення безпеки ключів [79].

Фактичний зміст проявляється через технічні дії, такі як ініціювання та підтвердження транзакцій, майнінг та валідація блоків, створення та виконання смарт-контрактів [80]. Важливу роль відіграють також організаційні дії, пов'язані з управлінням цифровими активами, взаємодією з іншими учасниками та забезпеченням технічної інфраструктури [81].

Співвідношення юридичного та фактичного змісту характеризується тісною взаємозалежністю, де фактичні дії породжують юридичні наслідки, а юридичні права реалізуються через технічні можливості [82]. Особливостями реалізації є автоматичне виконання через смарт-контракти, незворотність здійснених операцій та децентралізований характер взаємодії [83].

Порівняльно-правовий аналіз змісту інформаційних відносин у різних юрисдикціях виявляє суттєві відмінності у підходах до регулювання. Сінгапурська модель характеризується гнучким підходом до регулювання блокчейн-відносин, де основна увага приділяється захисту прав споживачів при збереженні простору для інновацій. Швейцарський підхід базується на чіткому розмежуванні різних типів цифрових активів та відповідній диференціації регуляторних вимог. Японська система відзначається комплексним регулюванням з акцентом на забезпечення кібербезпеки та захист персональних даних [69].

Глибинний міждисциплінарний аналіз блокчейн-відносин розкриває їх складну природу. В економічному аспекті спостерігається трансформація традиційних бізнес-моделей та поява нових форм монетизації цифрових активів. Соціологічні дослідження демонструють зміну патернів довіри у цифровому середовищі, де технологічні рішення починають відігравати роль соціальних інститутів. Технологічний розвиток створює можливості для автоматизації правовідносин, одночасно породжуючи виклики для традиційних механізмів регулювання [2].

Специфічні риси змісту інформаційних відносин у блокчейні проявляються через технологічну обумовленість, що включає залежність від коду, необхідність криптографічного захисту та вимоги до інфраструктури [37]. Правова специфіка полягає у поєднанні традиційних та нових правових конструкцій, необхідності адаптації класичних інститутів права та формуванні нових правових механізмів [76].

Глобальний характер блокчейн-відносин проявляється у їх транскордонності, необхідності міжнародної координації та виникненні проблем колізійного регулювання [23]. Це створює додаткові виклики для правового регулювання та вимагає розробки нових підходів до захисту прав учасників.

Таким чином, зміст інформаційних відносин у блокчейні являє собою складну систему взаємопов'язаних елементів, що поєднує юридичні права та обов'язки з їх технічною реалізацією в децентралізованому середовищі. Розуміння цієї специфіки є ключовим для формування ефективного правового регулювання блокчейн-відносин.

Права учасників блокчейн-відносин формуються на перетині технологічних можливостей та правових норм, створюючи особливу систему повноважень у цифровому середовищі. Специфіка цих прав зумовлена як технічними особливостями блокчейну, так і новими формами цифрової взаємодії [37, 76].

Ключовим елементом системи прав є право на володіння та розпорядження цифровими активами. Це право реалізується через можливість зберігання, передачі та використання криптовалют, токенів та інших віртуальних активів. Важливо відзначити, що фактична реалізація цього права безпосередньо пов'язана з доступом до приватних ключів, без яких здійснення операцій з активами стає неможливим [82].

Право на конфіденційність та захист інформації в блокчейн-середовищі має специфічний характер. У публічних блокчейнах всі транзакції є загальнодоступними, проте учасники можуть зберігати псевдонімність, використовуючи криптографічні адреси замість персональних даних. Додаткові механізми захисту, такі як змішувачі (mixers, сервіси для підвищення анонімності транзакцій) або приватні транзакції, дозволяють підвищити рівень конфіденційності [84].

Особливе значення має право на винагороду за підтримку мережі. Учасники, які забезпечують валідацію транзакцій через майнінг або стейкінг, отримують право на

винагороду у вигляді нових монет та комісій за транзакції. Це право є основою економічної мотивації для підтримки функціонування блокчейн-мережі [85].

Право на доступ до інформації в блокчейні реалізується по-різному залежно від типу мережі. В публічних блокчейнах кожен учасник має право переглядати всю історію транзакцій та стан рахунків. У приватних мережах це право може бути обмежене відповідно до правил системи. Консорціумні блокчейни часто використовують гібридний підхід, де учасники мають різний рівень доступу [86].

Важливим є право на участь у прийнятті рішень щодо розвитку мережі. В багатьох блокчейн-системах учасники можуть голосувати за зміни протоколу, оновлення мережі та інші рішення. Це право реалізується через механізми управління та є важливим елементом децентралізованої природи блокчейну [87].

Специфічним правом є можливість створення та використання смарт-контрактів. Учасники можуть програмувати автоматичне виконання різних умов, створювати DApps та використовувати наявні смарт-контракти. Це право трансформує традиційні договірні відносини, переводячи їх у цифрову площину [23].

Важливим аспектом є також право на правовий захист у блокчейн-середовищі. Традиційні механізми вирішення спорів трансформуються при застосуванні блокчейн-технологій, з'являються децентралізовані арбітражні системи та спеціалізовані процедури. Користувачі повинні мати гарантії захисту своїх прав у випадку технічних збоїв, атак на мережу або шахрайських дій інших учасників [88].

Всі ці права існують у контексті технологічних обмежень та правового регулювання різних юрисдикцій. Їх реалізація часто вимагає балансу між технологічною свободою та регуляторними вимогами, особливо в питаннях ідентифікації користувачів та протидії відмиванню коштів [76].

Таким чином, система прав учасників блокчейн-відносин являє собою складний комплекс можливостей, що поєднує технологічні інновації з правовими механізмами. Розуміння та ефективна реалізація цих прав є ключовим елементом розвитку блокчейн-екосистеми та її правового регулювання.

Обов'язки учасників блокчейн-відносин формують важливий компонент змісту інформаційних відносин, забезпечуючи стабільність та безпеку функціонування

децентралізованої системи. Ці обов'язки виникають як з технічних вимог самої технології, так і з правових норм різних юрисдикцій [89].

Фундаментальним обов'язком всіх учасників є дотримання мережевих протоколів та правил консенсусу. В публічних блокчейнах це означає необхідність формування транзакцій відповідно до встановлених стандартів, участь у процедурах оновлення протоколу та дотримання загальних правил взаємодії. Порушення цих вимог може призвести до відхилення транзакцій або виключення з мережі [85].

Виконання фінансових зобов'язань становить інший важливий аспект. Учасники зобов'язані сплачувати комісії за проведення транзакцій, які забезпечують економічну мотивацію для майнерів та валідаторів. У мережах з підтримкою смарт-контрактів особливого значення набуває концепція gas fees - оплати за обчислювальні ресурси, необхідні для виконання контрактів [87].

Значна увага приділяється обов'язкам щодо забезпечення безпеки. Учасники повинні зберігати конфіденційність своїх приватних ключів, використовувати надійні методи зберігання криптографічних даних та вживати заходів для захисту від несанкціонованого доступу. Втрата приватного ключа може призвести до безповоротної втрати доступу до активів [76].

У сфері регуляторних вимог основним є обов'язок дотримання KYC/AML. Хоча блокчейн початково орієнтований на анонімність, сучасні вимоги законодавства багатьох країн передбачають необхідність ідентифікації користувачів, особливо при взаємодії з централізованими платформами та фінансовими установами [90].

Особливого значення набувають обов'язки учасників, які забезпечують функціонування мережі. Майнери та валідатори зобов'язані підтримувати необхідну обчислювальну інфраструктуру, забезпечувати стабільність роботи вузлів та дотримуватися правил валідації транзакцій. Порушення цих обов'язків може призвести до втрати можливості отримання винагороди [23].

У контексті смарт-контрактів виникають специфічні обов'язки щодо коректності програмного коду та забезпечення його належного функціонування. Розробники несуть відповідальність за якість написання контрактів, а користувачі зобов'язані правильно взаємодіяти з ними відповідно до встановлених параметрів [86].

Важливим аспектом є обов'язки щодо розкриття інформації. У випадку здійснення ICO або випуску токенів організатори зобов'язані надавати повну та достовірну інформацію про проєкт, розкривати потенційні ризики та забезпечувати прозорість використання залучених коштів [37].

Аналіз міжнародної практики регулювання обов'язків учасників блокчейн-відносин демонструє тенденцію до посилення вимог щодо забезпечення прозорості та підзвітності. Особливої уваги заслуговує практика впровадження механізмів саморегулювання через професійні асоціації та галузеві стандарти.

Емпіричні дослідження дотримання регуляторних вимог у блокчейн-індустрії виявляють кореляцію між чіткістю нормативних вимог та рівнем їх виконання. Статистика порушень вказує на необхідність вдосконалення системи моніторингу та контролю, особливо у сфері протидії відмиванню коштів та захисту персональних даних. Це обґрунтовує доцільність впровадження автоматизованих систем комплаєнс-контролю (системи контролю за дотриманням регуляторних вимог) на основі технології блокчейн.

Таким чином, система обов'язків учасників блокчейн-відносин являє собою комплексний механізм, що забезпечує функціонування децентралізованої системи та захист прав усіх залучених сторін. Ефективне виконання цих обов'язків є необхідною умовою для розвитку та легітимації блокчейн-технологій у правовому полі.

Принципи децентралізації та автономності є фундаментальними характеристиками блокчейн-технології, що визначають особливості формування та реалізації інформаційних відносин. Сутність децентралізації полягає у відсутності єдиного центру управління та контролю. На відміну від традиційних систем, у блокчейні всі зміни та операції вимагають досягнення консенсусу між учасниками мережі, формуючи новий тип відносин, де довіра базується на математичних алгоритмах та колективній участі [87].

Децентралізація проявляється через розподілене зберігання даних, колективну валідацію транзакцій та механізми прийняття рішень щодо змін у протоколі. Принцип автономності реалізується через механізм смарт-контрактів, які виконуються

автоматично при настанні визначених умов. Це створює новий рівень правовідносин, де виконання зобов'язань забезпечується програмним кодом [76].

Реалізація прав у блокчейн-середовищі безпосередньо пов'язана з технологічними особливостями. Право власності на цифрові активи реалізується через володіння приватними ключами, а втрата ключа означає фактичну втрату можливості розпоряджатися активами. Це формує нову парадигму реалізації майнових прав, де технічний аспект стає визначальним [85].

Виконання обов'язків у блокчейні часто має автоматизований характер. Це проявляється у необхідності дотримання мережевих протоколів, сплаті комісій за транзакції та забезпеченні безпеки криптографічних ключів. Особливістю є те, що недотримання технічних вимог автоматично унеможливлює участь у мережі [91].

Важливим аспектом є взаємодія принципів децентралізації з вимогами регуляторів. Виникає необхідність пошуку балансу між збереженням переваг технології та забезпеченням відповідності правовим нормам. Це особливо важливо у питаннях ідентифікації користувачів та протидії відмиванню коштів [92].

Глобальний характер блокчейн-відносин створює додаткові виклики у визначенні застосовного права та юрисдикції. Учасники можуть знаходитися в різних країнах, що породжує питання колізійного регулювання. При цьому технічні протоколи залишаються єдиними для всіх учасників незалежно від їх місцезнаходження [86].

Вплив децентралізації на трансформацію правових механізмів проявляється у кількох ключових аспектах.

По-перше, змінюється природа правового захисту. У традиційній системі захист прав забезпечується державним примусом, тоді як у блокчейні - технологічними протоколами та економічними стимулами. Це вимагає розробки нових підходів до забезпечення прав учасників, де технічні механізми стають первинними гарантами виконання зобов'язань [90].

По-друге, трансформується система доказування. Якщо раніше достовірність інформації встановлювалася через складну систему доказів, то в блокчейні вона

забезпечується криптографічними механізмами та незмінністю розподіленого реєстру. Це створює нову парадигму доведення юридичних фактів [93].

По-третє, виникає феномен "програмованого права", де правові норми безпосередньо вбудовані в технологічну інфраструктуру через смарт-контракти. Це розмиває межу між правовими нормами та технічними протоколами, створюючи новий тип регулювання суспільних відносин.

Така трансформація правових механізмів вимагає переосмислення базових юридичних концепцій та розробки нових підходів до правового регулювання. Особливої уваги потребує питання співвідношення технологічних обмежень та правових норм, а також розробка механізмів вирішення конфліктів між програмним кодом та традиційним правом.

Порівняльно-правовий аналіз змісту блокчейн-відносин демонструє:

- - Різні підходи до визначення прав та обов'язків учасників
- - Відмінності в механізмах захисту прав
- - Специфіку реалізації принципу децентралізації

Аналіз змісту інформаційних відносин у блокчейн-середовищі та механізмів реалізації прав і обов'язків учасників створює методологічну основу для комплексного дослідження регуляторних підходів у наступних розділах. Розуміння специфіки децентралізованих взаємодій є ключовим для розробки ефективних механізмів правового регулювання та захисту прав учасників, що буде детально розглянуто в Розділах 2-4.

Міждисциплінарні дослідження впливу децентралізації на правовідносини демонструють трансформацію механізмів досягнення консенсусу та вирішення конфліктів. Соціологічні спостереження фіксують формування нових моделей довіри, базованих на математичних алгоритмах замість традиційних інституцій [37].

Аналіз сучасного стану інформаційних відносин у сфері блокчейн-технологій дозволяє визначити основні напрями їх подальшого розвитку.

Трансформація моделей взаємодії учасників блокчейн-відносин характеризується поступовим переходом від централізованих до гібридних моделей

управління. Розвиток нових форм цифрової ідентифікації та верифікації створює підґрунтя для більш надійних механізмів встановлення довіри. Поширення DAO формує нову парадигму корпоративного управління, а інтеграція блокчейну з технологіями штучного інтелекту та Інтернету речей (далі також – "IoT") відкриває нові можливості для автоматизації процесів.

Еволюція правового регулювання спрямована на формування спеціалізованого законодавства для блокчейн-сфери. Особливого значення набуває розвиток механізмів транскордонного регулювання та створення нових форм захисту прав учасників. Гармонізація національних та міжнародних норм стає необхідною умовою для ефективного функціонування глобальної блокчейн-екосистеми.

Розвиток технологічної інфраструктури характеризується впровадженням більш енергоефективних механізмів консенсусу та вдосконаленням масштабованості мереж. Розвиток рішень другого рівня спрямований на оптимізацію продуктивності, а посилення механізмів безпеки та приватності відповідає більшим вимогам користувачів та регуляторів.

Трансформація фінансового сектору відбувається через розвиток DeFi та впровадження цифрових валют центральних банків (далі також – "CBDC"). Інтеграція традиційних та криптофінансових інструментів створює можливості для інвестування та кредитування, змінюючи усталені фінансові парадигми.

Соціально-економічні зміни проявляються у формуванні нових моделей цифрової економіки та розвитку механізмів цифрового самоврядування. Трансформація моделей довіри та співпраці супроводжується створенням нових форм цифрової зайнятості та соціальної взаємодії.

Основними викликами залишаються необхідність балансування між інноваціями та безпекою, розв'язання проблем масштабованості та енергоефективності. Особливої уваги потребують питання захисту персональних даних та протидії використанню технології в незаконних цілях.

Інституційний розвиток характеризується формуванням спеціалізованих регуляторних органів та розвитком механізмів саморегулювання галузі. Створення

нових форм міжнародної співпраці та вдосконалення механізмів вирішення спорів стає необхідною умовою для сталого розвитку блокчейн-екосистеми.

Зазначені перспективи розвитку створюють контекст для детального аналізу приватно-правових аспектів, вивчення міжнародного досвіду регулювання та розробки рекомендацій щодо вдосконалення українського законодавства, що буде здійснено в наступних розділах дисертації. Особливої уваги потребує врахування цих тенденцій при формуванні національної стратегії розвитку блокчейн-технологій та відповідного правового регулювання.

ВИСНОВКИ ДО РОЗДІЛУ 1

1. Комплексне застосування різних наукових методів (історико-правового, порівняльно-правового, системного, формально-логічного) дозволило встановити системні зв'язки між технічними та правовими аспектами блокчейну, виявити специфіку правового статусу суб'єктів та об'єктів, порівняти різні підходи до регулювання та створити методологічну основу для подальшого дослідження міжнародного досвіду.

2. Дослідження інформаційних відносин у контексті блокчейн-технології демонструє фундаментальну трансформацію традиційних концепцій інформаційного права. Блокчейн створює нову парадигму децентралізованого зберігання та обробки даних, де достовірність інформації забезпечується не авторитетом джерела, а математичними алгоритмами та колективною верифікацією.

3. Аналіз технічних аспектів функціонування блокчейну виявив ключові характеристики технології (незмінність даних, криптографічний захист, розподілене зберігання, механізми консенсусу), які безпосередньо впливають на формування правового регулювання. Комплексне дослідження суб'єктного складу розкрило різноманітність учасників блокчейн-відносин та обґрунтувало неможливість визнання смарт-контрактів суб'єктами правовідносин.

4. Аналіз об'єктів інформаційних відносин у блокчейні виявив їх комплексну природу та різноманітність форм: від транзакційних даних до різних видів цифрових

активів (криптовалюти, токени, NFT) та смарт-контрактів. Кожен з цих об'єктів характеризується специфічними ознаками та потребує особливого правового режиму.

5. Дослідження змісту правовідносин у блокчейн-середовищі виявило специфіку реалізації прав та обов'язків учасників в умовах децентралізації. Встановлено, що технологічні особливості блокчейну (незмінність записів, автоматичне виконання смарт-контрактів) трансформують традиційні механізми реалізації прав та виконання обов'язків, створюючи нові виклики для правового регулювання.

6. На основі дослідження сформульовано ключові теоретичні положення щодо розвитку регулювання блокчейн-технологій, зокрема необхідність забезпечення балансу між технологічними особливостями та правовими механізмами, розробки спеціальних норм щодо статусу учасників та режиму об'єктів. Перспективи подальших досліджень пов'язані з аналізом приватно-правових механізмів, вивченням міжнародного досвіду та розробкою рекомендацій щодо вдосконалення національного законодавства.

Р О З Д І Л 2. Блокчейн-технології у приватно-правових відносинах

2.1. Приватно-правове регулювання та цивільно-правова природа блокчейн-правочинів

Застосування блокчейн-технологій у приватно-правових відносинах вимагає переосмислення традиційних методів правового регулювання. На відміну від публічно-правової сфери, що характеризується домінуванням імперативного методу регулювання, приватне право ґрунтується на засадах диспозитивності та автономії волі учасників правовідносин [15, 16]. Ця особливість набуває нового значення в контексті децентралізованих систем, де учасники самостійно визначають умови взаємодії через програмний код та смарт-контракти.

Основним методом приватно-правового регулювання блокчейн-відносин виступає координаційний метод, що передбачає рівність учасників та можливість самостійно визначати умови правовідносин. У блокчейн-середовищі це проявляється через свободу вибору контрагентів та платформ, можливість визначати умови смарт-контрактів, а також самостійне встановлення порядку виконання зобов'язань [14, 95].

Домінування координаційного методу зумовлено самою природою технології розподіленого реєстру, де учасники самостійно визначають параметри взаємодії. На відміну від традиційних цивільно-правових відносин, де координація часто опосередковується третіми особами (реєстраторами, нотаріусами тощо), у блокчейні вона реалізується безпосередньо через програмний код та криптографічні механізми [14]. Це створює новий рівень автономії учасників, але водночас вимагає від них вищого рівня відповідальності та технічної компетентності. Наприклад, при використанні смарт-контрактів сторони самостійно визначають умови їх виконання, які потім автоматично реалізуються без можливості одностороннього втручання [95].

Метод правонаділення забезпечує учасникам можливість набувати суб'єктивні цивільні права та обов'язки щодо віртуальних активів. Особливістю є те, що права часто фіксуються безпосередньо в блокчейні через криптографічні механізми [26, 27].

При цьому специфіка правонаділення в блокчейн-середовищі полягає у тому, що суб'єктивні права часто невіддільні від технічної можливості їх реалізації. Наприклад,

право розпорядження криптоактивами нерозривно пов'язане з володінням приватним ключем, а корпоративні права в DAO реалізуються через механізми цифрового голосування [26]. Така технологічна обумовленість правонаділення створює додаткові гарантії реалізації прав, але водночас вимагає особливої уваги до питань безпеки та захисту приватних ключів [27].

Своєю чергою, метод дозволу надає учасникам можливість здійснювати будь-які дії, які не заборонені. У контексті блокчейну це означає можливість створювати нові види віртуальних активів, розробляти інноваційні договірні конструкції та встановлювати особливі механізми забезпечення виконання зобов'язань [18, 38].

Межі методу дозволу в блокчейн-середовищі визначаються не лише правовими нормами, але й технічними можливостями та обмеженнями. Учасники можуть вчиняти будь-які дії, які технічно можливі та прямо не заборонені законом, однак ці дії повинні відповідати базовому протоколу та правилам конкретної платформи. Наприклад, створення нових токенів дозволено в межах, визначених стандартами відповідного блокчейну, а їх обіг може бути обмежений вимогами KYC/AML та податковими зобов'язаннями [18, 94].

Специфіка приватно-правового регулювання блокчейн-відносин проявляється у поєднанні традиційних цивілістичних принципів із технологічними можливостями децентралізованих систем. Принцип свободи договору (ст. 627 ЦКУ) реалізується через можливість сторін самостійно обирати види смарт-контрактів та умови їх виконання [2, 69]. Принцип добросовісності набуває нового змісту в контексті незмінності блокчейн-записів та автоматичного виконання зобов'язань [91, 96].

Особливу роль відіграє саморегулювання учасників, яке доповнює формальні методи правового регулювання. Воно проявляється через формування стандартів поведінки в мережах, розробку типових смарт-контрактів та протоколів взаємодії, а також створення механізмів вирішення спорів всередині спільноти [66, 97].

Практика саморегулювання в блокчейн-спільноті реалізується через різні механізми. На технічному рівні — це процедури консенсусу щодо оновлення протоколів та впровадження стандартів. На організаційному рівні — створення галузевих асоціацій та розробка кодексів поведінки. На операційному рівні —

формування типових договірних конструкцій та протоколів взаємодії [66]. Особливо ефективним є саморегулювання у сфері DeFi, де спільнота самостійно розробляє та впроваджує стандарти ліквідності, механізми управління ризиками та протоколи взаємодії між різними платформами [96].

Водночас приватно-правове регулювання блокчейн-відносин має враховувати публічні інтереси, зокрема щодо захисту прав споживачів, запобігання відмиванню коштів та забезпечення економічної безпеки [67, 96]. Це створює необхідність пошуку балансу між приватною автономією та публічними обмеженнями.

Суттєвою особливістю методів приватно-правового регулювання в блокчейн-середовищі є їх транскордонний характер. Учасники можуть знаходитися в різних юрисдикціях, що вимагає гнучких підходів до визначення застосовного права та механізмів захисту прав [96, 97]. При цьому технологічна специфіка блокчейну забезпечує правила взаємодії незалежно від географічного розташування учасників.

Таким чином, методи приватно-правового регулювання блокчейн-відносин характеризуються поєднанням диспозитивності та технологічної специфіки децентралізованих систем, що створює унікальний правовий режим для реалізації інтересів учасників цивільного обороту. Ефективність такого регулювання залежить від здатності правової системи адаптуватися до нових форм цифрової взаємодії при збереженні базових принципів приватного права [98].

Розглянувши особливості методів приватно-правового регулювання, доцільно проаналізувати співвідношення приватного та публічного регулювання у блокчейні.

Блокчейн-технології створюють новий контекст взаємодії приватного та публічного регулювання, де традиційні межі між цими сферами стають менш чіткими [14, 16]. Приватно-правові механізми, засновані на автономії волі та рівності сторін, взаємодіють із публічно-правовими вимогами щодо безпеки, прозорості та контролю.

Взаємодія приватних та публічних інтересів у блокчейн-середовищі детермінована іманентними характеристиками технології розподіленого реєстру. Блокчейн втілює ідею максимальної свободи та незалежності від централізованого контролю, проте повна анонімність створює ризики для публічних інтересів. При цьому властивості технології, зокрема транспарентність та незмінність даних,

одночасно виступають інструментом забезпечення публічного контролю та створюють перешкоди для його здійснення [14, 16].

Питання ідентифікації учасників блокчейн-відносин демонструє класичний конфлікт приватних та публічних інтересів. Якщо приватне право допускає анонімність при взаємній згоді сторін, то публічні інтереси вимагають впровадження процедур ідентифікації, особливо у фінансовій сфері [91, 99].

Співвідношення приватного та публічного регулювання проявляється також у питаннях захисту прав. Приватно-правові механізми захисту, такі як договірна відповідальність або відшкодування збитків, доповнюються публічно-правовими інструментами нагляду та контролю [66, 100]. При цьому природа блокчейну часто робить традиційні механізми державного примусу малоефективними, що вимагає розробки нових підходів до забезпечення балансу інтересів.

Використання смарт-контрактів може обмежуватися публічно-правовими нормами щодо певних сфер (наприклад, вимогами до ліцензування фінансових послуг або обмеженнями на обіг деяких видів активів) [18]. Крім того, автоматизований характер виконання смарт-контрактів вимагає особливих підходів до тлумачення волі сторін та застосування наслідків недійсності. Відтак, правова кваліфікація смарт-контрактів має враховувати як їх договірну природу, так і технологічну специфіку та публічно-правові обмеження [38].

Транскордонний характер блокчейн-технологій створює особливий контекст взаємодії приватного та публічного регулювання, де приватно-правові відносини легко долають кордони, тоді як публічно-правове регулювання залишається територіально обмеженим [37, 101]. Розв'язання цих проблем вимагає посилення міжнародної координації та гармонізації правових підходів, зокрема через розробку модельних правил та стандартів у сфері блокчейн-відносин на рівні міжнародних організацій та регіональних об'єднань [102].

У контексті розвитку блокчейн-технологій формується новий баланс між приватним та публічним регулюванням. Замість жорсткого протиставлення відбувається взаємне доповнення та посилення регуляторних механізмів. Приватно-

правові інструменти забезпечують гнучкість та інноваційність, тоді як публічно-правові норми створюють необхідні гарантії безпеки та стабільності [99, 100].

Отже, формування ефективного механізму правового регулювання блокчейн-відносин потребує комплексного підходу, що забезпечує органічну взаємодію приватно-правових та публічно-правових інструментів. Важливо забезпечити такий баланс, який дозволить максимально реалізувати потенціал технології, зберігаючи необхідний рівень захисту суспільних інтересів.

Беручи до уваги взаємодію приватного та публічного регулювання, важливо дослідити особливості реалізації принципу автономії волі в блокчейн-середовищі.

Принцип автономії волі, як фундаментальний принцип приватного права, набуває специфічного змісту в контексті блокчейн-відносин. У децентралізованому середовищі цей принцип трансформується, поєднуючи традиційні аспекти свободи волевиявлення із технологічними можливостями та обмеженнями [15, 16]. Специфіка проявляється в тому, що воля учасників часто виражається через взаємодію з програмним кодом та криптографічними механізмами.

Архітектурні особливості блокчейн-технології детермінують трансформацію механізмів реалізації автономії волі. Зокрема, волевиявлення учасників виражається через створення та підпис транзакцій за допомогою криптографічних ключів, а не через традиційні форми правочинів [15]. Крім того, воля сторін може бути зафіксована в смарт-контракті та автоматично реалізована при настанні закладених умов, без додаткового втручання суб'єктів [16]. Це підвищує ефективність та надійність виконання договорів, однак водночас обмежує можливості зміни або скасування волевиявлення через незмінність блокчейн-записів.

Автономія волі в блокчейн-середовищі проявляється насамперед у свободі вибору способу участі в децентралізованих відносинах. Учасники визначають, які платформи використовувати, які віртуальні активи придбавати, які смарт-контракти укладати [14, 99]. При цьому архітектура блокчейну забезпечує незалежність від централізованого контролю, що посилює реальну автономію учасників.

Водночас реалізація принципу автономії волі має певні особливості та обмеження. По-перше, як докладно проаналізовано в Розділі 2.1, після фіксації

транзакції в блокчейні "вона вважається виконаною остаточно і не може бути скасована або змінена в односторонньому порядку", що суттєво обмежує можливості зміни або скасування волевиявлення [26, 27]. По-друге, як встановлено в Розділі 2.1, використання смарт-контрактів передбачає автоматичне виконання закладених умов, незалежно від подальшого бажання учасників, що створює проблеми для "традиційних механізмів розірвання договору за згодою сторін або через суд" [18, 38].

Технічна незворотність блокчейн-транзакцій створює особливі правові наслідки для реалізації автономії волі. Як детально проаналізовано в Розділі 2.1, після запису транзакції в блокчейні її скасування або зміна стають практично неможливими, а автоматизація виконання смарт-контрактів, розглянута в Розділі 2.1, виключає можливість оперативного контролю. У зв'язку з цим необхідно на законодавчому рівні передбачити спеціальні механізми для виправлення помилок без порушення цілісності блокчейну.

Важливим аспектом є питання вираження волі через цифрові підписи та криптографічні ключі. У традиційному розумінні підпис документа свідчить про волевиявлення особи. У блокчейн-середовищі використання приватного ключа для підписання транзакції також розглядається як форма вираження волі, хоча і має свою специфіку [91, 96]. Втрата приватного ключа може фактично позбавити особу можливості реалізувати свою волю щодо розпорядження активами.

Використання цифрових підписів та криптографічних ключів як форми волевиявлення в блокчейні породжує питання про їх правову природу та співвідношення з традиційними концепціями. З одного боку, цифровий підпис, створений за допомогою приватного ключа, виконує класичні функції власноручного підпису, забезпечуючи ідентифікацію особи та підтвердження її волі [91]. З іншого боку, втрата приватного ключа фактично означає втрату можливості розпорядження цифровими активами, що ставить під сумнів реальність волевиявлення [96]. Відтак, правове регулювання використання цифрових підписів повинно враховувати їх технологічну специфіку та передбачати особливі механізми відновлення контролю над ключами та верифікації дійсності волевиявлення.

Реалізація принципу автономії волі нерозривно пов'язана з проблематикою визначення правосуб'єктності учасників блокчейн-відносин. Учасники можуть діяти анонімно або псевдонімно, що створює певні виклики для встановлення дійсної волі сторін та їх правоздатності [66, 103]. Особливо це актуально при вирішенні спорів, коли необхідно встановити, чи дійсно особа мала намір вчинити певні дії в блокчейні.

Анонімність учасників блокчейн-відносин створює проблему верифікації їх правосуб'єктності як умови дійсності правочинів. Адже без надійної ідентифікації сторін складно встановити їх право- та дієздатність, а також реальність волевиявлення [66]. Це породжує ризики укладення недійсних правочинів або зловживань з боку недобросовісних учасників. Розв'язання зазначеної проблеми потребує впровадження децентралізованих систем ідентифікації, які забезпечують верифікацію суб'єкта правовідносин за умови збереження конфіденційності його персональних даних [103]. Крім того, важливим є законодавче визначення статусу анонімних транзакцій та розробка презумпцій дійсності правочинів за певних умов.

У контексті міжнародних відносин автономія волі в блокчейн-середовищі набуває додаткового виміру. Учасники наділені правом вибору застосовного права та юрисдикції, однак технологічна природа блокчейну створює певні обмеження у реалізації таких виборів [67, 104]. Наприклад, виконання судового рішення може бути ускладнене через технічну неможливість змінити записи в блокчейні.

DAO демонструє нові форми реалізації волі учасників. У таких організаціях воля формується та виражається через механізми цифрового голосування та автоматичного виконання рішень [69]. Це створює новий рівень автономії, де правила взаємодії визначаються не лише договірними умовами, але й кодом.

Проведений аналіз ключових аспектів приватно-правового регулювання блокчейн-відносин дає підстави для таких висновків.

Принцип автономії волі в блокчейн-середовищі, зберігаючи свою фундаментальну роль у приватному праві, набуває нових форм реалізації та обмежень. Технологічна специфіка блокчейну створює унікальні можливості для вираження та реалізації волі учасників, але водночас вимагає переосмислення традиційних підходів до розуміння волевиявлення та його правових наслідків.

Отже, формування ефективного механізму правового регулювання блокчейн-відносин потребує збалансованого поєднання приватно-правових та публічно-правових інструментів. Такий баланс має забезпечувати реалізацію потенціалу технології та автономію учасників, водночас створюючи достатні гарантії захисту суспільних інтересів та стабільності цивільного обороту.

Розглянуті загальні засади приватно-правового регулювання блокчейн-відносин створюють основу для аналізу конкретних цивільно-правових механізмів, насамперед правочинів, що здійснюються у цифровому середовищі.

Першочергового значення набуває дослідження природи правочинів у блокчейн-середовищі, оскільки саме вони є основною формою реалізації приватної автономії учасників цивільного обороту.

Наявність волевиявлення сторін є однією з ключових ознак правочину відповідно до цивільного законодавства [7]. Водночас у контексті блокчейн-транзакцій процес волевиявлення характеризується певною специфікою, що зумовлена технічними особливостями технології [3].

По-перше, волевиявлення учасників блокчейн-транзакцій реалізується через використання криптографічних ключів, що виконують функцію цифрових підписів [27]. Кожен учасник має свою унікальну пару ключів — публічний та приватний. Публічний ключ використовується для ідентифікації учасника, а приватний — для підписання транзакцій від його імені. Таким чином, сам факт підписання транзакції приватним ключем свідчить про наявність відповідного волевиявлення сторони.

Водночас втрата приватного ключа фактично позбавляє особу можливості розпоряджатися своїми віртуальними активами, навіть за наявності у неї іншим чином підтвердженого права власності. Це створює ризики безповоротної втрати доступу до цифрових об'єктів та ускладнює захист прав власників у таких випадках [105]. Відтак, правове регулювання блокчейн-транзакцій повинно передбачати механізми відновлення контролю над втраченими ключами та врахування технічних аспектів при тлумаченні змісту волевиявлення сторін.

По-друге, процес обміну волевиявленнями в блокчейн-середовищі зазвичай відбувається без безпосередньої взаємодії сторін, а через протокол [106]. Після

підписання транзакція транслюється в мережу, де вона перевіряється та включається в блокчейн іншими учасниками. Відтак, сторони можуть не мати прямого контакту між собою, а їх воля опосередковується технічною інфраструктурою.

Ці особливості зумовлюють певні складнощі щодо тлумачення змісту та спрямованості волі сторін блокчейн-правочинів, зокрема в аспекті ідентифікації суб'єктів волевиявлення з огляду на часткову анонімність учасників блокчейн-мереж [26]. Крім того, автоматизований характер виконання транзакцій ускладнює оцінку справжності волі та наявності вад волевиявлення.

Відтак, приватно-правове регулювання блокчейн-відносин повинно враховувати специфіку волевиявлення в цифровому середовищі. Зокрема, це вимагає формування підходів до ідентифікації, перевірки автентичності волі, а також тлумачення змісту правочинів з урахуванням технічного контексту. Ефективне розв'язання цих питань є однією з передумов інтеграції блокчейн-технологій у цивільно-правову сферу.

Розглянувши специфіку волевиявлення в цифровому середовищі, доцільно проаналізувати особливості автоматизації виконання зобов'язань через смарт-контракти.

Якщо в Розділі 1 увага приділялася технічним аспектам смарт-контрактів, то в рамках приватно-правового регулювання фокус зміщується на особливості їх використання як договірного інструменту. Основною проблемою є співвідношення автоматизованого виконання з класичними принципами договірного права — свободою договору, автономією волі та можливістю захисту порушених прав.

Важливим аспектом є правова кваліфікація смарт-контрактів. З позиції приватного права, вони є формою фіксації домовленостей сторін [62, 82]. Однак публічне право може встановлювати окремі вимоги щодо форми, змісту та порядку їх виконання, особливо коли вони стосуються регульованих видів діяльності.

Важливим аспектом є момент виникнення договірних зобов'язань при використанні смарт-контрактів. Якщо в традиційних договорах цей момент зазвичай пов'язаний з досягненням згоди щодо всіх істотних умов, то в смарт-контрактах необхідно враховувати як момент погодження умов, так і момент розміщення програмного коду в блокчейні [90].

Особливої уваги заслуговує питання зміни або розірвання смарт-контракту. Традиційні механізми розірвання договору за згодою сторін або через суд стикаються з технічною неможливістю зупинити виконання вже запущеного смарт-контракту. Це вимагає розробки спеціальних механізмів, таких як включення в код можливості призупинення виконання або створення процедур компенсації наслідків автоматичного виконання [81].

Специфіка цивільно-правової відповідальності за порушення смарт-контракту полягає в необхідності розмежування відповідальності за некоректне програмування умов та відповідальності за невиконання зобов'язань. При цьому важливо досягти забезпечення судового захисту прав, навіть якщо смарт-контракт вже виконано [36].

Перспективи розвитку договірних механізмів з використанням смарт-контрактів пов'язані з розробкою гібридних форм, що поєднують автоматизоване виконання з можливістю гнучкого реагування на зміну обставин та захисту інтересів сторін.

Беручи до уваги роль смарт-контрактів у блокчейн-середовищі, важливо дослідити загальні вимоги до форми та умов дійсності блокчейн-правочинів.

Цивільне законодавство встановлює загальні вимоги до форми правочинів та умов їх дійсності [7]. В контексті блокчейн-транзакцій ці вимоги набувають певних особливостей, обумовлених технічною специфікою середовища.

Щодо форми правочинів, блокчейн-транзакції за своєю природою вчиняються в електронній формі. При цьому електронна форма часто розглядається як специфічний різновид письмової форми [83]. Так, інформація про транзакції фіксується у вигляді записів в розподіленому реєстрі, які криптографічно підписуються сторонами. Відтак, блокчейн забезпечує виконання основних функцій письмової форми — достовірну фіксацію змісту правочину та ідентифікацію сторін, що його вчинили.

Водночас використання електронної форми в блокчейн-середовищі породжує і певні проблеми. Зокрема, виникають питання щодо визначення моменту вчинення правочину, його місця, а також забезпечення доступності та цілісності електронних записів у довгостроковій перспективі [26]. Ці аспекти вимагають вироблення спеціальних правових підходів та технічних стандартів.

Щодо умов дійсності правочинів, загальні вимоги цивільного права (законність змісту, дієздатність сторін, вільне волевиявлення тощо) залишаються актуальними й для блокчейн-транзакцій. Однак і тут є певні нюанси. Наприклад, анонімність учасників блокчейн-мереж ускладнює верифікацію їх дієздатності та встановлення умислу. Крім того, автоматизований характер смарт-контрактів породжує питання щодо оцінки відповідності їх змісту вимогам законодавства [91].

Без належної ідентифікації сторін складно визначити, чи володіють вони необхідним обсягом право- та дієздатності для вчинення конкретного правочину. Крім того, анонімність ускладнює тлумачення змісту правочинів та встановлення дійсної волі сторін у разі виникнення спорів [66]. Розв'язання цих проблем може потребувати розвитку децентралізованих систем ідентифікації учасників або встановлення спеціальних правових презумпцій.

Ще однією проблемою є забезпечення вільного волевиявлення сторін в умовах технічної стандартизації блокчейн-протоколів. Адже умови блокчейн-транзакцій часто диктуються не стільки сторонами, скільки технічною інфраструктурою. Це створює ризики нав'язування невигідних умов та обмеження свободи договору [37].

Відтак, приватно-правове регулювання блокчейн-відносин повинно забезпечити адаптацію загальних вимог до форми та дійсності правочинів до технічних реалій. Зокрема, це передбачає визначення статусу електронної форми, вироблення механізмів ідентифікації, перевірки змісту смарт-контрактів, а також забезпечення вільного волевиявлення. Розв'язання цих питань дозволить повноцінно використовувати переваги блокчейну зі збереженням цивільно-правових гарантій.

Проаналізувавши ключові аспекти блокчейн-правочинів, необхідно звернути увагу на практичні проблеми реституції та "скасування" транзакцій.

Однією з визначальних рис блокчейну є незмінність та безвідкличність проведених транзакцій [27]. З технічного погляду, після включення транзакції до блокчейну вона вважається виконаною остаточно і не може бути скасована або змінена в односторонньому порядку. Ця особливість створює виклик для традиційних цивільно-правових механізмів, спрямованих на відновлення початкового становища сторін у випадку визнання правочину недійсним або його розірвання.

Зокрема, класичний інститут реституції, який передбачає повернення сторін у початкове становище шляхом повернення всього отриманого за недійсним правочином [7], стикається з практичною неможливістю "скасування" блокчейн-транзакцій. Адже з технічного погляду блокчейн просто не передбачає можливості вилучення або заміни вже записаної інформації [8].

Ця проблема загострюється з огляду на децентралізований характер більшості блокчейн-мереж, де відсутній єдиний центр контролю, який міг би санкціонувати зміну записів на виконання рішення суду або іншого компетентного органу. Відтак, навіть за наявності законних підстав для застосування реституції, її практична реалізація в блокчейн-середовищі є вкрай ускладненою.

Така ситуація склалася, наприклад, у резонансній справі The DAO, де через помилку в коді зловмисник зміг вивести значну суму коштів, а повернення цих коштів виявилося технічно неможливим та потребувало додаткових дій з боку розробників платформи Ethereum [46]. Цей випадок демонструє необхідність розробки правових та технічних механізмів реституції для блокчейн-відносин.

Одним із можливих шляхів розв'язання цієї проблеми є застосування зворотних транзакцій для фактичного повернення сторін у початкове становище. Наприклад, якщо первісна транзакція передбачала переказ коштів, зворотна транзакція може передбачати переказ цих коштів у зворотному напрямку. Однак такий підхід має свої недоліки, адже він не скасовує первісну транзакцію, а лише компенсує її [66].

Іншим варіантом є використання різного роду ескроу-механізмів (система умовного депонування, при якій цифрові активи блокуються до виконання заздалегідь визначених умов) та мультипідписних рахунків (спеціальний криптовалютний рахунок, що вимагає підписів декількох приватних ключів для здійснення транзакції), які дозволяють відкласти фактичне виконання транзакції до настання певних умов або досягнення згоди між сторонами [92]. Однак ці механізми повинні бути закладені в смарт-контракт від самого початку, що не завжди можливо.

Відтак, проблема реституції та "скасування" транзакцій в блокчейн-середовищі потребує комплексного підходу. Він має поєднувати відповідні технічні рішення на рівні протоколів та смарт-контрактів з адаптацією правових механізмів до реалій

блокчейну. Зокрема, це може передбачати перегляд підходів до визнання правочинів недійсними, розробку альтернативних способів відновлення становища, а також вироблення стандартів зворотності транзакцій для різних типів блокчейн-систем.

Розглянуті особливості блокчейн-правочинів безпосередньо впливають на специфіку договірних механізмів, що використовуються у цифровому середовищі та потребують детального аналізу.

Блокчейн-технології відкривають нові можливості для реалізації договірних відносин, забезпечуючи надійність, прозорість та ефективність. Водночас застосування блокчейну в договірній сфері характеризується низкою особливостей, що зумовлюють необхідність адаптації цивільно-правових механізмів. Договірні механізми, спираючись на загальні принципи блокчейн-правочинів, створюють конкретні правові інструменти для регулювання відносин між учасниками.

Для розуміння специфіки договірних механізмів у блокчейн-середовищі необхідно насамперед проаналізувати особливості укладення та виконання договорів.

Укладення договорів у блокчейн-середовищі характеризується поєднанням традиційних юридичних стадій (оферта та акцепт) з технічними аспектами створення та підписання транзакцій. При цьому важливо розмежовувати момент досягнення згоди щодо істотних умов та момент технічної фіксації договору в блокчейні [36].

Наприклад дуалістична природа смарт-контрактів проявляється в тому, що вони одночасно є і правочином (домовленістю сторін), і способом його виконання (через автоматизований код). З погляду приватного права, смарт-контракти підпадають під загальні вимоги до форми та змісту договорів [62].

Договірні механізми в блокчейн-середовищі характеризуються специфічними рисами, що впливають на всі стадії договірного процесу. На стадії переддоговірних відносин особливого значення набуває питання ідентифікації сторін та перевірки їх дієздатності. При цьому традиційні механізми перевірки контрагента повинні бути адаптовані до умов цифрового середовища.

Момент укладення договору в блокчейн-середовищі може визначатися по-різному залежно від обраного сторонами способу взаємодії. Якщо при традиційному укладенні договору таким моментом вважається досягнення згоди щодо всіх його

істотних умов, то в цифровому середовищі не менш важливого значення набуває технічна фіксація цієї згоди в розподіленому реєстрі.

Особливістю договірних механізмів у блокчейн-середовищі є також можливість поєднання традиційних договірних конструкцій з автоматизованим виконанням окремих умов. Це створює гібридні форми договірних відносин, де частина умов може виконуватися автоматично, а частина — потребувати активних дій сторін.

Важливим аспектом є питання зміни та припинення договірних відносин. Якщо в традиційних договорах сторони мають відносну свободу в модифікації умов за взаємною згодою, то в блокчейн-середовищі така можливість може бути технічно обмежена, що вимагає особливої уваги до формулювання початкових умов договору.

Особливістю блокчейн-договорів є можливість їх самовиконання за допомогою смарт-контрактів. Так, умови договору можуть бути закладені в код, який автоматично виконується при настанні певних умов [86]. Це дозволяє мінімізувати ризики, пов'язані з людським фактором, а також забезпечити швидкість та ефективність виконання зобов'язань.

Водночас автоматизація виконання договорів через смарт-контракти породжує і проблеми. Зокрема, виникають питання щодо можливості внесення змін або розірвання договору в односторонньому порядку, а також забезпечення тлумачення умов договору в разі виникнення спорів [91]. Адже смарт-контракти виконуються автоматично і не передбачають можливості втручання або перегляду результатів.

Іншим аспектом є забезпечення конфіденційності умов договору та персональних даних сторін в умовах публічності блокчейну. Адже за замовчуванням інформація в блокчейні є відкритою та доступною для всіх учасників мережі. Відтак, постає необхідність у використанні додаткових механізмів шифрування або обмеження доступу до чутливої інформації [89].

Важливим напрямом практичного застосування договірних механізмів у блокчейн-середовищі є управління ланцюгами поставок. Використання блокчейн-технологій дозволяє забезпечити простежуваність товарів від виробника до споживача, що підвищує рівень довіри між учасниками та зменшує ризики. Показовим є досвід компанії Walmart, яка впровадила блокчейн-систему для

відстеження походження м'ясних та плодоовочевих продуктів [107]. Ця система значно пришвидшила процес ідентифікації джерела походження товарів та підвищила ефективність логістичних процесів.

Підсумовуючи, укладення та виконання договорів у блокчейн-середовищі має свою специфіку, обумовлену технічними особливостями технології. З одного боку, блокчейн дозволяє підвищити ефективність та надійність договірних відносин, автоматизувати виконання зобов'язань та мінімізувати ризики. З іншого боку, його використання вимагає адаптації традиційних договірних механізмів, вироблення нових підходів до тлумачення та зміни умов договорів, а також забезпечення належного рівня конфіденційності. Ефективне розв'язання цих питань є запорукою успішної інтеграції блокчейну в договірні відносини.

Розглянувши специфіку укладення та виконання блокчейн-договорів, доцільно перейти до аналізу їх основних видів та класифікації.

Розвиток блокчейн-технологій та поширення віртуальних активів зумовлює появу нових видів договорів, які потребують належної класифікації та правового регулювання. Зокрема, можна виділити кілька основних типів договорів, що укладаються в блокчейн-середовищі:

1. Договори купівлі-продажу віртуальних активів (токенів, криптовалют тощо). Ці договори передбачають передачу права власності на певну кількість віртуальних активів в обмін на традиційні валюти або інші віртуальні активи, що зумовлює виникнення питань щодо правового статусу таких активів, порядку їх обліку, оподаткування та захисту прав споживачів [66, 108].
2. Договори про надання послуг, пов'язаних з віртуальними активами. Це можуть бути договори про зберігання віртуальних активів (наприклад, на криптовалютних біржах або гаманцях), договори про надання послуг з обміну віртуальних активів, а також договори про надання консультаційних, інформаційних або технічних послуг у сфері блокчейну [67, 109].
3. Інвестиційні договори (договори про краудфандинг, ICO тощо). Ці договори передбачають залучення інвестицій у формі віртуальних активів для реалізації певних проєктів або створення нових блокчейн-платформ. При цьому інвестори

отримують право на частку майбутнього прибутку або інші права, пов'язані з реалізацією проєкту [48, 51]. Водночас такі договори потребують чіткого правового регулювання для захисту прав інвесторів та запобігання шахрайству.

4. Ліцензійні договори щодо використання блокчейн-технологій або розподілених реєстрів. Ці договори передбачають надання прав на використання певних блокчейн-протоколів, смарт-контрактів або інших технологічних рішень в обмін на ліцензійні платежі [80, 110]. При цьому важливо забезпечити належний захист прав інтелектуальної власності та врегулювати питання відповідальності за якість і безпеку відповідних технологій.
5. Договори про створення та використання токенізованих активів. Йдеться про договори, спрямовані на оцифрування традиційних активів (нерухомості, цінних паперів, прав вимоги тощо) шляхом створення їх аналогів (токенів) на блокчейні [52, 111]. Такі договори дозволяють підвищити ліквідність та доступність відповідних активів, однак потребують належного правового регулювання для захисту прав власників та запобігання зловживанням.

У практиці використання віртуальних активів сформувалася низка типових договірних конструкцій, що застосовуються учасниками цивільного обороту. Аналіз практики їх використання дозволяє виділити кілька основних видів договорів.

Договори купівлі-продажу віртуальних активів становлять базову категорію правочинів у блокчейн-середовищі. Їх особливістю є специфічна форма передачі прав на цифрові активи через транзакції в розподіленому реєстрі, що забезпечує одночасність передачі активу та отримання зустрічного надання [18, 112].

Договори зберігання цифрових активів спрямовані на забезпечення професійного зберігання та управління віртуальними активами. Особливістю таких договорів є регламентація порядку управління приватними ключами, розподілу ризиків втрати доступу та процедур відновлення контролю над активами [27, 105].

Договори про участь у пулах ліквідності передбачають об'єднання цифрових активів кількох учасників для забезпечення функціонування DeFi-протоколів. Специфіка цих договорів полягає у встановленні механізмів розподілу винагороди між учасниками та правил управління активами [18, 113].

Договори стейкінгу є особливою формою участі в забезпеченні роботи блокчейн-мережі через блокування певної кількості активів. Характерною рисою таких договорів є поєднання умов про термін блокування активів з механізмами участі в валідації транзакцій та отримання відповідної винагороди [31, 33].

Запропонована класифікація має не лише теоретичне, але й важливе практичне значення, оскільки визначає особливості правового режиму різних видів договорів та специфіку захисту прав їх сторін. Зокрема, це впливає на порядок виконання зобов'язань, розподіл ризиків між сторонами та механізми вирішення спорів.

Наведена класифікація не є вичерпною і може доповнюватися новими видами договорів з розвитком блокчейн-технологій. Відтак, важливим завданням є розробка гнучких правових рамок, здатних адаптуватися до динамічних змін у цій сфері. Зокрема, це передбачає визначення правового статусу віртуальних активів, встановлення вимог до форми та змісту відповідних договорів, а також створення ефективних механізмів захисту прав сторін. Належне регулювання договірних відносин у блокчейн-середовищі дозволить підвищити правову визначеність та стимулювати розвиток інноваційних бізнес-моделей.

Беручи до уваги різноманітність договорів з віртуальними активами, важливо дослідити особливості забезпечення виконання зобов'язань у блокчейн-середовищі.

Блокчейн-технології відкривають можливості для забезпечення виконання зобов'язань, дозволяючи мінімізувати ризики їх невиконання або неналежного виконання. Зокрема, можна виділити кілька основних механізмів забезпечення виконання зобов'язань у блокчейн-середовищі, окрім смарт-контрактів [36, 79].

Традиційні способи забезпечення виконання зобов'язань у контексті віртуальних активів набувають специфічних рис.

Застава віртуальних активів характеризується особливим механізмом фіксації обтяження та порядком звернення стягнення. На відміну від традиційної застави, де предмет часто залишається у володінні заставодавця, при заставі віртуальних активів найбільш ефективним є їх переміщення на спеціальний рахунок або мультипідписний гаманець. Це забезпечує неможливість розпорядження без згоди заставодержателя [64, 114].

Порука в цифровому середовищі може реалізовуватися через спеціальні протоколи гарантування, де поручитель забезпечує виконання зобов'язань через блокування власних цифрових активів. При цьому важливо чітко визначити механізм реалізації відповідальності поручителя та порядок стягнення забезпечення.

Гарантія як спосіб забезпечення може використовуватися у формі цифрових гарантійних зобов'язань, які автоматично виконуються при настанні визначених умов. Особливістю є необхідність чіткої формалізації умов настання гарантійного випадку та механізму виплати гарантійної суми [81, 86].

Притримання права на віртуальні активи реалізується через технічні механізми блокування доступу до активів до моменту виконання зобов'язань боржником. Ефективність цього способу забезпечення значно підвищується завдяки неможливості обходу технічних обмежень.

Розвиток цифрового середовища сприяв появі нових форм забезпечення виконання зобов'язань, які не мають аналогів у традиційному цивільному обороті.

Токенізоване забезпечення передбачає створення спеціальних токенів, які представляють право вимоги щодо забезпечувального активу. Такі токени можуть вільно обертатися на вторинному ринку, при цьому базовий актив залишається заблокованим до моменту виконання основного зобов'язання [112, 115].

Протоколи ліквідації забезпечення дозволяють автоматично реалізувати забезпечення через децентралізовані аукціони при порушенні умов. Особливістю є прозорість процедури та відсутність необхідності звернення до судових органів [18, 113].

Децентралізовані протоколи кредитування використовують механізм надлишкового забезпечення, коли вартість заблокованих цифрових активів повинна перевищувати суму зобов'язання на визначений коефіцієнт. При зниженні вартості забезпечення нижче встановленого рівня відбувається автоматична ліквідація позиції [53, 70].

Репутаційне забезпечення базується на системах оцінки надійності учасників, де порушення зобов'язань призводить до зниження репутаційного рейтингу та обмеження можливостей подальшої участі в цифровому економічному обороті.

Смарт-контракти як інструмент забезпечення виконання зобов'язань мають ряд специфічних особливостей застосування в цивільному обороті.

У забезпечувальній функції смарт-контракти можуть використовуватися кількома способами. По-перше, як механізм автоматичного блокування активів до виконання зустрічних зобов'язань. По-друге, як інструмент автоматичного виконання забезпечувальних зобов'язань при порушенні основного договору. По-третє, як спосіб фіксації та реалізації забезпечувальних прав [62, 82].

При використанні смарт-контрактів у забезпечувальних механізмах важливо чітко визначити:

- - Умови та момент блокування забезпечення
- - Порядок перевірки виконання забезпечених зобов'язань
- - Механізм реалізації забезпечення у разі порушення
- - Можливість оскарження автоматичного виконання

Увагу слід приділити питанню судового контролю за реалізацією забезпечення через смарт-контракти. Необхідно передбачити можливість втручання у випадках, коли виконання може призвести до порушення прав сторін або третіх осіб.

Серед технічних механізмів забезпечення виконання зобов'язань у блокчейн-середовищі основними є: мультипідписні транзакції, що вимагають схвалення декількох учасників; депонування коштів через смарт-контракти; автоматизовані системи умовного виконання [41, 45].

Ці механізми дозволяють створити додаткові гарантії належного виконання зобов'язань, використовуючи особливості блокчейну. Важливим механізмом забезпечення є токенізація активів, яка дозволяє автоматизувати передачу прав на реальні активи через блокчейн при виконанні встановлених умов [66, 116].

Вибір конкретних механізмів забезпечення має враховувати не лише технічні можливості блокчейн-платформи, але й правові наслідки їх застосування. Особливо важливим є забезпечення балансу між автоматизацією виконання та можливістю судового контролю за реалізацією забезпечувальних механізмів.

Наведені механізми дозволяють істотно підвищити рівень виконання договірних зобов'язань у блокчейн-середовищі та мінімізувати ризики невиконання або неналежного виконання. Водночас їх використання потребує належного правового забезпечення. Зокрема, необхідно визначити правовий статус смарт-контрактів та токенізованих активів, врегулювати порядок використання мультипідписних рахунків та ескроу, а також забезпечити можливість судового захисту прав сторін у разі виникнення спорів. Ефективне поєднання технічних та правових інструментів дозволить розкрити потенціал блокчейну як надійного механізму забезпечення виконання договірних зобов'язань.

Проаналізувавши механізми забезпечення виконання зобов'язань, необхідно звернути увагу на проблеми розподілу ризиків та відповідальності сторін у блокчейн-договорах.

Попри переваги використання блокчейн-технологій в договірних відносинах, їх застосування пов'язане з певними ризиками та проблемами розподілу відповідальності між сторонами. Ці питання потребують ретельного правового аналізу та вироблення збалансованих підходів.

Система ризиків та відповідальності в блокчейн-середовищі охоплює кілька ключових категорій:

1. Технічні ризики: збої в роботі блокчейн-платформ та смарт-контрактів; помилки в програмному коді; втрата або компрометація приватних ключів; несанкціонований доступ до цифрових активів [20, 46, 53].
2. Економічні ризики: волатильність вартості віртуальних активів; зміна економічного балансу договору; ризики ліквідності цифрових активів; курсові різниці при транскордонних операціях [47, 107].
3. Юридичні ризики: невизначеність правового статусу окремих видів операцій; складність визначення застосовного права; проблеми судового захисту прав; ризики регуляторних обмежень [67, 99, 103].
4. Механізми розподілу відповідальності: договірне закріплення розподілу ризиків між сторонами; встановлення лімітів відповідальності; використання страхових механізмів; впровадження технічних засобів контролю [113, 117].

Ефективне управління цими ризиками вимагає комплексного підходу, що поєднує правові механізми розподілу відповідальності з технічними засобами забезпечення безпеки операцій. При цьому особливого значення набуває чітке договірне регулювання питань відповідальності сторін за різні категорії ризиків.

Окремої уваги потребують питання відповідальності за недійсність або незаконність договорів, укладених у блокчейні. Враховуючи транскордонний характер блокчейн-транзакцій, може виникати ситуація, коли договір є дійсним за правом однієї юрисдикції, але недійсним або незаконним за правом іншої [68, 112]. Відтак, важливо забезпечити механізми перевірки відповідності договорів вимогам застосовного права та передбачити наслідки їх недійсності.

При розподілі ризиків необхідно враховувати специфіку блокчейн-середовища, де традиційні підходи до визначення вини та причинно-наслідкового зв'язку можуть бути неефективними. Це створює необхідність розробки спеціальних критеріїв розподілу відповідальності, що враховували б як технічні особливості блокчейну, так і загальні принципи договірного права.

Підсумовуючи, розподіл ризиків та відповідальності сторін у блокчейн-середовищі потребує комплексного підходу, який враховував би особливості технології, економічні реалії ринку віртуальних активів, а також специфіку транскордонних відносин. Зокрема, необхідно виробити підходи до розподілу відповідальності за технічні збої та помилки, передбачити механізми розподілу курсових ризиків, врегулювати наслідки втрати приватних ключів, а також забезпечити відповідність договорів вимогам застосовного права. Ефективне розв'язання цих питань на рівні практики та законодавчого регулювання дозволить мінімізувати правові ризики та стимулювати подальший розвиток блокчейн-індустрії.

Аналіз договірних механізмів природно приводить до необхідності дослідження питань права власності на віртуальні активи, що виступають об'єктом цих договірних відносин.

2.2. Право власності та цивільно-правовий захист у блокчейн-відносинах

Специфіка реалізації права власності в цифровому середовищі має суттєвий вплив на характер та зміст договірних конструкцій.

Широке використання блокчейну та віртуальних активів породжує низку питань щодо правового режиму власності. Зокрема, необхідно визначити, якою мірою традиційні концепції речового права можуть бути застосовані до цифрових об'єктів, а також які особливості притаманні відносинам власності у блокчейн-середовищі.

Дослідження права власності на цифрові активи передбачає насамперед аналіз специфіки їхньої правової природи та реалізації правомочностей власника.

Цифрові активи, включаючи криптовалюти, токени та NFT, становлять особливий вид майна, що характеризується унікальними властивостями та потребує адаптації традиційних цивілістичних підходів.

Віртуальні активи як об'єкти цивільних прав характеризуються здатністю втілювати різні види майнових прав — від класичного права власності до корпоративних прав у DAO. При цьому ключовою особливістю є відсутність матеріального субстрату та залежність реалізації прав від володіння криптографічними ключами [102].

Однією з ключових особливостей цифрових активів є відсутність їх матеріального субстрату. На відміну від традиційних об'єктів права власності (рухомих та нерухомих речей), віртуальні активи існують виключно у цифровій формі і не мають фізичного втілення [112, 116]. Це створює складнощі для застосування класичної тріади правомочностей власника (володіння, користування, розпорядження), яка розроблялася з орієнтацією на матеріальні речі.

Зокрема, виникає питання, у чому саме полягає володіння віртуальними активами? З технічного погляду, володіння криптовалютами або токенами зводиться до можливості доступу до відповідного запису в блокчейні за допомогою приватного ключа [27]. Однак чи можна вважати такий доступ повноцінним володінням з погляду речового права? Адже фактично відсутня фізична влада над річчю, яка традиційно вважалася невіддільною ознакою володіння.

При цьому різні види цифрових активів мають свою специфіку: криптовалюти функціонують як засоби обміну та накопичення, утилітарні токени надають доступ

до послуг або прав, а NFT забезпечують унікальність та незамінність об'єктів [73, 115].

Іншим аспектом є можливість одночасного володіння віртуальним активом кількома особами. Враховуючи, що запис у блокчейні може бути скопійований та доступний одночасно багатьом користувачам, виникає питання про визначення "справжнього" власника активу [63]. Це вимагає вироблення спеціальних правових механізмів фіксації та захисту прав власності у блокчейн-середовищі.

Ця особливість найбільш яскраво проявляється у випадку з мультипідписними гаманцями та смарт-контрактами, де контроль над активом може бути розподілений між кількома учасниками за заздалегідь визначеними правилами.

Ще однією особливістю є неможливість повного контролю над віртуальними активами з боку держави або інституцій. Враховуючи характер більшості блокчейн-мереж, відсутні технічні можливості для примусового вилучення або обмеження обігу віртуальних активів за рішенням суду або інших компетентних органів [87]. Це створює ризики для використання віртуальних активів у протиправних цілях та ускладнює застосування традиційних механізмів правового захисту.

Водночас розвиток технологій і регуляторних підходів відкриває нові можливості для забезпечення прозорості й контрольованості операцій із цифровими активами зі збереженням їхніх основних переваг як об'єктів права власності [118]. Зокрема, технології відстеження транзакцій та ідентифікації користувачів дозволяють забезпечувати баланс між приватністю та регуляторними вимогами.

Підсумовуючи, володіння віртуальними активами має низку особливостей, які відрізняють його від володіння традиційними об'єктами права власності. Зокрема, воно характеризується відсутністю фізичного субстрату, можливістю одночасного доступу кількох осіб, а також обмеженими можливостями контролю з боку централізованих інституцій. Ці особливості створюють виклики для адаптації традиційних концепцій речового права до реалій блокчейн-середовища та вимагають вироблення нових правових підходів. Ефективне розв'язання цих питань є необхідною передумовою для розвитку обороту віртуальних активів та захисту прав їх власників.

Таким чином, особливості володіння цифровими активами зумовлюють необхідність розробки спеціальних правових механізмів, які б враховували технологічну специфіку різних видів віртуальних активів та забезпечували ефективний захист прав їх власників. Це особливо важливо в контексті способів фіксації та передачі прав, що буде розглянуто далі.

Проаналізувавши особливості володіння цифровими активами, необхідно звернути увагу на способи юридичної фіксації та передачі прав на такі активи.

Блокчейн-технології пропонують нові способи фіксації та передачі прав на віртуальні активи, які відрізняються від традиційних механізмів, притаманних матеріальним об'єктам. Зокрема, права на віртуальні активи фіксуються через створення відповідних записів у розподіленому реєстрі, доступ до яких здійснюється за допомогою криптографічних ключів [92].

Передача прав на віртуальні активи здійснюється через створення незмінного запису в розподіленому реєстрі, що забезпечує прозорість та достовірність історії переходів права власності. Особливістю криптовалютних транзакцій є їх безпосередній характер, без опосередкування фінансовими установами [11].

Специфіка реалізації правомочностей власника щодо цифрових активів проявляється у:

- володінні через контроль криптографічних ключів;
- користуванні шляхом здійснення транзакцій та отримання вигод;
- розпорядженні через передачу прав іншим учасникам [26, 27].

В контексті смарт-контрактів фіксація права власності набуває особливого значення. Автоматизоване виконання умов контракту та передача прав створюють нову реальність, де технічна можливість розпорядження активом прирівнюється до юридичного титулу власності. Це вимагає розробки спеціальних механізмів захисту прав власників у випадках технічних збоїв або втрати доступу до активів.

Водночас виникає питання щодо юридичної кваліфікації таких способів фіксації та передачі прав. Чи можна вважати запис у блокчейні повноцінним правовстановлюючим документом, що підтверджує право власності на актив? Яким

чином співвідносяться традиційні вимоги до форми правочинів (проста письмова, нотаріальне посвідчення тощо) з фіксацією прав у блокчейні? Ці питання потребують ретельного дослідження та вироблення відповідних правових позицій.

Традиційні способи розпорядження майновими правами адаптуються до специфіки блокчейн-середовища через механізми смарт-контрактів, що забезпечують автоматизовану передачу прав при настанні визначених умов [18, 36].

Ще одним важливим питанням є захист прав добросовісних набувачів віртуальних активів. Враховуючи анонімність більшості блокчейн-транзакцій, існують ризики придбання активів, які походять від незаконної діяльності або були набуті з порушенням прав третіх осіб [53, 119]. Відтак, важливо виробити критерії визначення добросовісності набувачів та передбачити механізми захисту їх прав у разі витребування активів законними власниками.

Способи фіксації та передачі прав на віртуальні активи мають свою специфіку, обумовлену особливостями блокчейн-технологій. Хоча технічна інфраструктура блокчейну забезпечує надійність та прозорість обліку прав, її юридична імплементація потребує вирішення низки теоретичних та практичних питань. Зокрема, необхідно визначити правову природу записів у блокчейні, адаптувати традиційні договірні конструкції до потреб обороту віртуальних активів, а також забезпечити захист прав добросовісних набувачів. Ефективне розв'язання цих питань дозволить створити цілісну та несуперечливу систему обліку та передачі прав власності у блокчейн-середовищі.

Розглянувши механізми фіксації прав на віртуальні активи, логічно перейти до аналізу способів захисту права власності у блокчейн-середовищі.

Ефективний захист права власності на віртуальні активи є ключовою умовою для розвитку блокчейн-індустрії та зміцнення довіри учасників ринку. Водночас специфіка блокчейн-технологій створює певні виклики для традиційних механізмів захисту права власності, що вимагає вироблення нових підходів та рішень.

Застосування традиційного віндикаційного позову до віртуальних активів ускладнюється специфікою блокчейну: анонімністю учасників, відсутністю унікальної ідентифікації активів та швидкістю зміни їх власників [7, 120].

Система захисту права власності на віртуальні активи включає три рівні:

1. Превентивні механізми: використання мультипідписних гаманців; розподіл активів між різними сховищами; регулярний аудит безпеки [66].
2. Договірні механізми: умовне депонування активів страхування ризиків; арбітражні застереження [64].
3. Процесуальні механізми: судовий захист порушених прав; звернення до регуляторних органів; альтернативне вирішення спорів [25].

Ефективність захисту забезпечується комплексним застосуванням цих механізмів з урахуванням специфіки конкретної ситуації."

Особливої складності набуває захист прав власників криптовалют. Специфіка криптовалют як децентралізованих активів створює унікальні виклики для традиційних механізмів захисту. По-перше, незворотність транзакцій унеможливлює примусове повернення криптовалют без згоди фактичного володільця приватного ключа. По-друге, транскордонний характер операцій ускладнює визначення юрисдикції для захисту порушених прав. По-третє, анонімність або псевдонімність учасників створює складнощі у встановленні належного відповідача [47, 53].

Практика показує, що найбільш ефективними є превентивні механізми захисту прав власників криптовалют: використання мультипідписних гаманців, зберігання криптовалют на регульованих платформах з системами страхування, застосування додаткових засобів аутентифікації. При цьому важливо забезпечити баланс між безпекою зберігання та зручністю використання криптовалют у цивільному обороті.

Іншим поширеним способом захисту є негаторний позов, тобто вимога про усунення перешкод у здійсненні права власності, не пов'язаних з позбавленням володіння [7]. У контексті блокчейн-середовища такі перешкоди можуть полягати, наприклад, у неправомірному доступі третіх осіб до приватних ключів власника або у здійсненні несанкціонованих транзакцій з його активами [27]. Однак ефективність негаторного захисту залежить від можливості ідентифікації порушника та доведення факту неправомірного втручання, що може бути проблематично в умовах блокчейну.

Ще одним механізмом захисту права власності є визнання транзакцій недійсними та застосування реституції [7]. Однак, як вже зазначалося, блокчейн за своєю природою не передбачає можливості скасування або зміни транзакцій. Відтак, застосування реституції можливе лише шляхом вчинення нових зворотних транзакцій, які компенсують наслідки недійсних правочинів [99]. При цьому виникають ризики порушення прав добросовісних набувачів віртуальних активів.

З огляду на це, ефективний захист права власності у блокчейні потребує комплексного підходу, який передбачає поєднання правових та технічних механізмів. З правового погляду, необхідно адаптувати традиційні способи захисту до специфіки віртуальних активів, зокрема, шляхом вироблення критеріїв ідентифікації об'єктів та суб'єктів права власності, встановлення презумпцій добросовісності набуття, а також розробки процедур розгляду спорів у блокчейні.

З технічного погляду, важливо забезпечити надійність та безпеку блокчейн-інфраструктури, зокрема, шляхом удосконалення механізмів зберігання приватних ключів, запровадження багатофакторної автентифікації (система підтвердження особи користувача, що вимагає надання двох або більше доказів автентичності з різних категорій: знання (паролі), володіння (токени, смартфони) та біометричні дані) користувачів, а також розробки стандартів безпеки для смарт-контрактів [20]. Крім того, перспективним напрямом є використання страхових механізмів для компенсації збитків власників віртуальних активів у разі їх втрати або викрадення [67].

У контексті захисту прав власників криптовалют важливого значення набуває розвиток спеціалізованих механізмів вирішення спорів. Це може включати створення експертних центрів з технічної експертизи блокчейн-транзакцій, розробку процедур відновлення доступу до криптовалютних гаманців, формування стандартів доказування права власності на криптовалюти.

Традиційні способи захисту права власності потребують суттєвої адаптації до специфіки віртуальних активів. Зокрема, виникає питання про можливість застосування віндикації у випадках несанкціонованого доступу до цифрових активів через компрометацію приватних ключів [66, 120]. При цьому важливо забезпечити захист прав власника з урахуванням обмежень блокчейн-систем.

Підсумовуючи, захист права власності на віртуальні активи є складним завданням, що потребує адаптації традиційних підходів до реалій блокчейн-середовища. Ефективне вирішення цього завдання передбачає поєднання правових та технічних механізмів, спрямованих на забезпечення надійності обліку прав, запобігання неправомірним втручанням, а також справедливе вирішення спорів. Розвиток відповідної правової та технічної інфраструктури є передумовою для сталого розвитку ринку віртуальних активів та захисту інтересів його учасників.

Окрім загальних питань захисту права власності, особливої уваги заслуговують проблеми спадкування віртуальних активів, які мають свою специфіку.

З розвитком блокчейн-технологій та зростанням обсягів віртуальних активів все більшої актуальності набувають питання їх спадкування. Адже віртуальні активи, такі як криптовалюти або токени, можуть становити значну майнову цінність, яка здатна входити до складу спадщини. Водночас специфіка блокчейн-середовища створює низку особливостей та проблем у сфері спадкового правонаступництва.

Спадкування віртуальних активів характеризується трьома основними проблемами:

1. Технічний аспект — необхідність передачі приватних ключів спадкоємцям при збереженні їх конфіденційності;
2. Правовий аспект — специфіка оформлення волі спадкодавця щодо цифрових активів;
3. Процедурний аспект — особливості включення віртуальних активів до складу спадщини.

Ще однією проблемою є забезпечення прав кредиторів спадкодавця у разі переходу віртуальних активів до спадкоємців. Адже віртуальні активи не мають чітких територіальних зв'язків та можуть бути легко виведені з-під контролю кредиторів [121]. Крім того, анонімність блокчейн-транзакцій ускладнює процес пошуку та ідентифікації віртуальних активів у складі спадщини. Це створює ризики порушення прав кредиторів та зловживань з боку недобросовісних спадкоємців.

Ефективне регулювання спадкування віртуальних активів вимагає поєднання технічних засобів захисту з правовими механізмами забезпечення прав спадкоємців та захисту інтересів кредиторів спадкодавця.

Для забезпечення ефективного спадкування віртуальних активів використовуються: смарт-контракти з функцією спадкування; довірче управління активами та механізми відкладеного доступу до приватних ключів [90, 113].

Підсумовуючи, спадкування віртуальних активів має низку особливостей, зумовлених технічними та правовими аспектами функціонування блокчейн-середовища. Для ефективного регулювання цих відносин необхідно виробити підходи до забезпечення передачі приватних ключів спадкоємцям, розробити механізми цифрових заповітів, забезпечити захист прав кредиторів, а також визначити порядок оподаткування віртуальних активів у складі спадщини. Належне розв'язання цих питань потребує підходу, який враховував би стандарти блокчейн-систем, досвід інших країн, а також практики спадкового планування.

Особливості реалізації права власності на віртуальні активи зумовлюють необхідність формування спеціальних механізмів цивільно-правового захисту, що враховували б специфіку цифрового середовища.

Імплементація блокчейн-технологій у приватно-правову сферу детермінує необхідність трансформації усталених механізмів захисту до особливостей функціонування розподіленого реєстру. Адже блокчейн-середовище характеризується низкою рис, таких як децентралізованість, криптографічна захищеність, незворотність транзакцій тощо, що створюють виклики для застосування звичних способів захисту прав. Традиційні механізми захисту потребують адаптації до умов цифрового середовища та особливостей віртуальних активів. Розглянемо основні способи захисту порушених прав у блокчейн-відносинах.

В блокчейн-середовищі основними способами захисту порушених прав виступають: визнання права на віртуальні активи; відновлення до них доступу; припинення неправомірних транзакцій та відшкодування збитків у криптовалюті [7].

Зокрема, визнання права власності на віртуальні активи або права вимоги за зобов'язаннями, що виникають зі смарт-контрактів, потребує чіткого визначення

правової природи відповідних об'єктів та розробки критеріїв їх ідентифікації [99]. Відновлення становища, яке існувало до порушення, може бути ускладнене у зв'язку з незворотністю транзакцій та неможливістю їх скасування в односторонньому порядку [122]. Припинення дії, яка порушує право, вимагає розробки технічних механізмів впливу на функціонування децентралізованих блокчейн-систем [26].

Ефективність захисту прав у блокчейн-середовищі визначається: технічною можливістю реалізації судових рішень; наявністю механізмів ідентифікації порушника; можливістю фактичного відновлення порушеного права [87, 113].

При цьому особливого значення набуває превентивна функція захисту, оскільки відновлення порушеного права може бути технічно ускладненим або неможливим.

Специфіка захисту прав у блокчейн-середовищі ускладнюється його транскордонним характером. Невідповідності в національному регулюванні різних юрисдикцій створюють додаткові виклики для ефективного судового захисту та виконання рішень [103]. Це вимагає розробки спеціальних механізмів міжнародної координації та гармонізації підходів до захисту прав учасників блокчейн-відносин.

Ще однією проблемою є забезпечення ефективного відшкодування збитків, завданих неправомірними діями в блокчейн-середовищі. Адже анонімність учасників блокчейн-транзакцій ускладнює ідентифікацію порушника та притягнення його до відповідальності [66]. Крім того, волатильність курсів віртуальних активів зумовлює складнощі в оцінці реальних збитків та визначенні розміру компенсації [67].

Таким чином, забезпечення ефективного захисту прав у блокчейн-відносинах зумовлює необхідність модифікації традиційних цивілістичних способів до технічних реалій розподіленого реєстру. Зокрема, це передбачає розробку механізмів ідентифікації віртуальних активів та прав на них, створення технічної можливості виконання судових рішень щодо транзакцій, а також формування підходів до оцінки та компенсації збитків з урахуванням особливостей віртуальних активів.

Ефективність застосування способів захисту прав безпосередньо залежить від можливості доведення обставин порушення. Відтак, особливої уваги заслуговують питання доказування у блокчейн-середовищі.

Реалізація механізмів цивільно-правового захисту нерозривно пов'язана з процесом доказування, який забезпечує встановлення фактичних обставин справи на підставі досліджених доказів. Доказування в блокчейн-середовищі базується на: криптографічних доказах здійснення транзакцій; даних розподіленого реєстру; технічній експертизі смарт-контрактів; електронних підписах учасників [92].

Однією з ключових особливостей є використання криптографічних доказів, тобто даних, що підтверджують існування певних фактів у блокчейні (наприклад, здійснення транзакції, укладення смарт-контракту тощо). З одного боку, такі докази забезпечують високий рівень достовірності та захищеності інформації, зафіксованої в розподіленому реєстрі. Водночас застосування таких доказів зумовлює необхідність використання спеціальних технічних знань та програмного забезпечення, що створює додаткові вимоги до кваліфікації учасників процесу та суду [3].

Іншим аспектом є забезпечення допустимості електронних доказів, отриманих з блокчейн-систем. Адже традиційні вимоги до форми та засвідчення доказів не завжди враховують технічну специфіку розподіленого реєстру. Зокрема, постає питання про визнання юридичної сили даних, зафіксованих у блокчейні, а також встановлення їх зв'язку з конкретними особами та обставинами справи.

Ще однією проблемою є визначення предмета доказування у спорах, що виникають з блокчейн-відносин. Адже традиційні юридичні факти, які потребують встановлення (укладення договору, передача майна, виконання зобов'язання тощо), можуть мати нетипове вираження в умовах розподіленого реєстру [18]. Крім того, анонімність блокчейн-транзакцій може значно ускладнювати процес встановлення реальних суб'єктів відносин та їх дій, що мають юридичне значення.

Використання цифрових доказів у спорах щодо віртуальних активів створює необхідність розробки стандартів їх допустимості та достовірності. Особливої уваги потребує питання встановлення автентичності цифрових доказів та їх зв'язку з конкретними суб'єктами [92, 110]. При цьому важливо забезпечити баланс між технічною достовірністю та можливістю їх оскарження у встановленому порядку.

Проведений аналіз свідчить, що процес доказування в блокчейн-середовищі характеризується специфічними рисами, зумовленими технічною специфікою

розподіленого реєстру. Для ефективного використання криптографічних та електронних доказів необхідно виробити спеціальні юридичні та технічні стандарти, які забезпечували б їх релевантність, допустимість та належність. Крім того, важливо переглянути традиційні підходи до визначення предмета доказування та розподілу обов'язків з доказування з урахуванням особливостей функціонування блокчейн-систем. Врахування цих аспектів при вирішенні спорів дозволить підвищити ефективність захисту прав учасників блокчейн-відносин.

Проаналізувавши специфіку доказування, необхідно звернути увагу на практичні механізми компенсації збитків, завданих порушенням прав.

Інститут відшкодування збитків як фундаментальний спосіб захисту цивільних прав забезпечує відновлення майнового становища особи, право якої порушено. Водночас застосування цього механізму в блокчейн-середовищі може стикатися з низкою практичних проблем, зумовлених технічними особливостями розподіленого реєстру та економічними властивостями віртуальних активів.

Першочергового вирішення потребує проблема динамічної зміни вартості віртуальних активів, що безпосередньо впливає на визначення обсягу реальних збитків. Адже через різкі коливання курсів криптовалют та токенів сума збитків, визначена на момент порушення права, може значно відрізнятися від суми, необхідної для відновлення майнового становища потерпілого на момент фактичного відшкодування [67, 107]. Це зумовлює потребу у виробленні спеціальних підходів до визначення розміру компенсації з урахуванням динаміки ринку віртуальних активів.

Особливої уваги заслуговує питання забезпечення практичної реалізації судових рішень щодо відшкодування збитків. Адже через децентралізований характер блокчейн-систем та анонімність учасників транзакцій може бути складно встановити місцезнаходження боржника та його активів, що підлягають стягненню [121]. Крім того, незворотність блокчейн-транзакцій унеможливлює примусове списання коштів з рахунків боржника без його волевиявлення [41]. Відтак, постає необхідність у розробці додаткових механізмів забезпечення виконання, таких як обмеження доступу до певних сервісів чи активів у разі ухилення від сплати компенсації.

Ще однією проблемою є відшкодування збитків, завданих внаслідок технічних помилок або вразливостей. Адже через автоматизований характер їх виконання помилки в коді можуть призводити до непередбачуваних наслідків та істотних втрат для учасників [46]. При цьому може бути складно визначити належного відповідача та довести його вину, особливо у випадку анонімних розробників смарт-контрактів. Це зумовлює потребу в розробці спеціальних правил відповідальності за дефекти смарт-контрактів, а також страхових механізмів компенсації відповідних збитків.

Визначення розміру збитків у блокчейн-відносинах потребує розробки спеціальних методик оцінки, які б враховували волатильність вартості віртуальних активів та специфіку цифрового середовища. Особливого значення набуває питання визначення причинно-наслідкового зв'язку між порушенням та збитками, особливо у випадках автоматизованого виконання смарт-контрактів [67, 91].

Підсумовуючи, відшкодування збитків у блокчейн-відносинах потребує врахування технічних та економічних особливостей розподіленого реєстру. Зокрема, необхідно виробити підходи до визначення розміру компенсації з урахуванням волатильності віртуальних активів, забезпечити ефективність виконання судових рішень в умовах децентралізованої інфраструктури, а також передбачити механізми відповідальності за дефекти смарт-контрактів та страхування відповідних ризиків. Розв'язання цих питань дозволить підвищити дієвість компенсаційних механізмів та забезпечити справедливий розподіл ризиків у блокчейн-середовищі.

Поряд із механізмами відшкодування збитків, важливе значення мають превентивні способи захисту, спрямовані на запобігання порушень прав.

У системі способів захисту цивільних прав превентивні механізми, поряд з відновлювальними та компенсаційними, набувають особливого значення, спрямовані на запобігання порушенням та мінімізацію відповідних ризиків. В контексті блокчейн-відносин превентивний захист набуває особливого значення, зважаючи на високий рівень автоматизації процесів та незворотність здійснених транзакцій.

Система превентивних способів захисту включає декілька рівнів:

1. Технічні механізми: багатофакторна автентифікація; моніторинг транзакцій; резервне копіювання ключів [20, 27].

2. Правові механізми: детальна регламентація прав сторін; процедури узгодження операцій; протоколи вирішення спорів [25, 26].
3. Організаційні заходи: внутрішній контроль; аудит; навчання учасників [50].

Особливе значення має превентивний захист прав споживачів, що включає:

- Розкриття повної інформації про особливості та ризики операцій.
- Надання детальних інструкцій щодо безпечного використання сервісів.
- Встановлення лімітів на операції для зниження ризиків.
- Впровадження процедур верифікації значних транзакцій.

Фундаментальним елементом превентивного захисту виступає забезпечення функціональної надійності та технічної безпеки блокчейн-систем. Це передбачає використання перевірених криптографічних протоколів, регулярне оновлення програмного забезпечення, а також проведення комплексних аудитів безпеки смарт-контрактів [44, 45]. Крім того, важливо забезпечити надійність інфраструктури зберігання приватних ключів, від яких залежить доступ до віртуальних активів та можливість ініціювання транзакцій [27]. Відповідні заходи дозволяють мінімізувати ризики несанкціонованого доступу, втрати даних та інших технічних загроз.

Наступним системоутворюючим елементом превентивного захисту є формування механізмів забезпечення прозорості та підзвітності суб'єктів. Зокрема, це передбачає розкриття інформації про умови смарт-контрактів, політику емісії токенів, а також про результати діяльності блокчейн-проектів [112]. Забезпечення транспарентності створює передумови для прийняття обґрунтованих рішень учасниками та мінімізації ризиків зловживань у системі. При цьому важливо забезпечити баланс між транспарентністю та захистом конфіденційної інформації, що може досягатися за допомогою спеціальних криптографічних механізмів [39].

Невіддільною частиною системи превентивного захисту є розвиток правової свідомості та підвищення рівня професійної компетентності учасників блокчейн-відносин. Адже значна частина порушень прав у цій сфері зумовлена необізнаністю користувачів щодо технічних та правових аспектів функціонування блокчейн-систем

[15]. Зазначене зумовлює необхідність імплементації комплексної системи інформаційно-освітніх заходів щодо роз'яснення правового статусу учасників, особливостей укладення та виконання смарт-контрактів, а також механізмів захисту порушених прав. Це дозволить попереджати типові помилки та підвищити загальний рівень правової свідомості в блокчейн-середовищі.

Ефективність превентивного захисту забезпечується комплексним застосуванням технічних, правових та організаційних механізмів з урахуванням специфіки конкретних блокчейн-платформ [19, 30].

Проведене дослідження демонструє, що превентивні способи захисту є визначальними для забезпечення стабільності функціонування та інституційної довіри до блокчейн-відносин. Вони спрямовані на запобігання порушень прав шляхом забезпечення технічної надійності систем, прозорості діяльності учасників, а також підвищення їх обізнаності щодо правових аспектів. Ефективне використання превентивних механізмів дозволяє мінімізувати ризики та створити більш сприятливе середовище для реалізації можливостей блокчейн-технологій. Водночас вони мають розглядатися не як альтернатива, а як важливе доповнення до компенсаційних та відновлювальних способів захисту порушених прав.

Ці способи захисту прав становлять частину інституту цивільно-правової відповідальності, який набуває особливого значення в контексті блокчейн-відносин.

2.3. Інститут цивільно-правової відповідальності

Цивільно-правова відповідальність у блокчейні базується на поєднанні традиційних підстав відповідальності з технологічними особливостями системи.

Підставами відповідальності в блокчейн-середовищі є:

1. Порушення умов смарт-контракту;
2. Неправомірне використання приватних ключів;
3. Недотримання протоколів безпеки;
4. Зловживання правами в децентралізованих системах [36, 91].

Аналіз підстав цивільно-правової відповідальності в блокчейн-середовищі виявляє специфічну трансформацію класичних елементів складу правопорушення. Протиправність діяння набуває особливого змісту в контексті автоматизованого виконання смарт-контрактів, а причинно-наслідковий зв'язок характеризується складною технологічною опосередкованістю. Водночас специфіка блокчейн-відносин зумовлює необхідність адаптації цих підстав до технічних та економічних реалій розподіленого реєстру, наприклад смарт-контрактів.

Основними формами відповідальності виступають:

1. Відшкодування збитків у криптовалюті;
2. Автоматизовані штрафні санкції через смарт-контракти;
3. Обмеження доступу до децентралізованих сервісів;
4. Примусова ліквідація позицій у DeFi-протоколах [67, 113].

У контексті безпідставного збагачення виникає потреба у формуванні нових підходів до кваліфікації набуття майна без достатньої підстави та визначення умов його повернення, враховуючи особливості цифрових активів та автоматизованого виконання операцій. Відтак, постає потреба в розробці умов та механізмів реституції безпідставного збагачення з урахуванням технічних особливостей блокчейну.

Аналіз специфіки цивільно-правової відповідальності у відносинах з віртуальними активами виявляє низку особливостей. По-перше, виникає проблема встановлення причинно-наслідкового зв'язку між порушенням та збитками в умовах автоматизованого виконання. Зокрема, коли збитки виникають внаслідок взаємодії кількох смарт-контрактів або через каскадний ефект в децентралізованих протоколах [46, 53].

По-друге, потребує уваги питання вини як умови відповідальності. Складність програмних систем та їх взаємодії може створювати ситуації, коли шкода виникає без явної вини конкретного учасника. Це вимагає розробки критеріїв для оцінки ступеня обачності та дбайливості учасників цивільного обороту в цифровому середовищі.

По-третє, виникає проблема визначення розміру збитків при операціях з волатильними цифровими активами. Суттєві коливання вартості віртуальних активів

створюють необхідність розробки методик оцінки реальних збитків та упущеної вигоди з урахуванням динаміки ринку [70, 107].

Специфічною рисою відповідальності в цій сфері є також необхідність розмежування відповідальності різних категорій учасників — користувачів, розробників, операторів платформ. Важливо встановити чіткі критерії для визначення меж відповідальності кожного учасника та випадків її обмеження.

Особливого значення набуває превентивна функція цивільно-правової відповідальності. Враховуючи складність або неможливість примусового виконання рішень щодо віртуальних активів, акцент має бути зроблений на запобіганні порушенням через створення ефективних механізмів забезпечення виконання зобов'язань та управління ризиками.

Компенсація збитків у блокчейн-середовищі здійснюється через: прямі компенсаційні виплати у криптовалюті; відновлювальні транзакції; страхові механізми; системи автоматичної компенсації через смарт-контракти [86, 113].

Підсумовуючи, при визначенні підстав цивільно-правової відповідальності в блокчейн-середовищі важливо враховувати особливості функціонування розподіленого реєстру та смарт-контрактів. Зокрема, це передбачає адаптацію традиційних умов договірної, деліктної та кондикційної відповідальності, а також вироблення спеціальних правил щодо розподілу ризиків та тягаря доказування. Ефективне регулювання цих питань дозволить забезпечити справедливий та збалансований розподіл відповідальності між учасниками блокчейн-відносин.

Цивільно-правова відповідальність може існувати в різних формах, кожна з яких має свою специфіку застосування. Серед основних форм відповідальності можна виділити відшкодування збитків, сплату неустойки та втрату завдатку.

Відшкодування збитків як основна форма відповідальності в цифровому середовищі потребує особливих механізмів реалізації. При визначенні розміру збитків важливо враховувати не лише прямі майнові втрати, але й специфічні види шкоди, характерні для операцій з віртуальними активами — втрату можливості використання цифрових активів, витрати на відновлення доступу до гаманців, збитки від вимушеного продажу активів у несприятливий момент.

При визначенні форм відповідальності важливо враховувати можливість їх реального застосування в умовах децентралізованої системи. Ефективність тієї чи іншої форми відповідальності значною мірою залежить від наявності технічних механізмів її реалізації та можливості примусового виконання. Це створює необхідність розробки нових форм відповідальності, які б органічно поєднувалися з технічною архітектурою блокчейн-систем.

Неустойка як форма відповідальності набуває нового змісту через можливість її автоматизованого нарахування та стягнення. При цьому важливо забезпечити відповідність розміру неустойки принципу співмірності та можливість її судового зменшення у виняткових випадках. Особливого значення набуває використання неустойки як способу стимулювання належної поведінки учасників.

Оперативно-господарські санкції у цифровому середовищі можуть включати обмеження доступу до певних функцій платформ, призупинення операцій з активами, блокування облікових записів. Важливо забезпечити прозорість застосування таких санкцій та можливість їх оскарження.

Новою формою відповідальності, специфічною для цифрового середовища, стає позбавлення або обмеження цифрових прав — наприклад, виключення з-поміж валідаторів, обмеження права голосу в DAO, зниження рівня довіри в репутаційних системах [63, 122]. Такі форми відповідальності потребують чіткого нормативного регулювання для запобігання зловживанням.

Компенсаційні виплати як форма відповідальності можуть використовуватися у випадках, коли точне визначення розміру збитків ускладнене. Наприклад, при порушенні прав користувачів цифрових платформ, у разі збоїв у роботі смарт-контрактів або при витоку конфіденційних даних.

Сплата неустойки (штрафу, пені) є спеціальною формою відповідальності, яка застосовується у випадках, передбачених договором або законом [7]. В контексті блокчейн-відносин неустойка може використовуватися як засіб стимулювання належного виконання смарт-контрактів. Зокрема, умови смарт-контракту можуть передбачати автоматичне списання визначеної суми з рахунку сторони у разі

порушення нею своїх зобов'язань [18]. При цьому важливо забезпечити, щоб розмір неустойки був розумним та співмірним із можливими збитками.

Втрата завдатку є особливою формою відповідальності, яка полягає у втраті стороною, яка надала завдаток, права на його повернення у разі невиконання нею договору [7]. В блокчейні завдаток може забезпечуватися шляхом депонування суми на спеціальному рахунку (ескроу), з якого вона автоматично переводиться іншій стороні у разі настання певних умов [39]. При цьому важливо чітко визначити підстави для втрати завдатку та забезпечити розподіл ризиків між сторонами.

Слід зазначити, що вибір конкретної форми відповідальності в блокчейн-відносинах має ґрунтуватися на врахуванні особливостей конкретних відносин, характеру можливих порушень, а також технічних можливостей їх реалізації. При цьому перевага має віддаватися тим формам, які найкраще забезпечують баланс інтересів сторін та мінімізують ризики зловживань.

Важливо також враховувати, що форми відповідальності в блокчейн-середовищі можуть комбінуватися та доповнювати одна одну. Наприклад, умови смарт-контракту можуть передбачати як автоматичну сплату неустойки за прострочення виконання, так і відшкодування підтверджених збитків на вимогу сторони [27].

Інститут цивільно-правової відповідальності в блокчейн-середовищі продовжує розвиватися, адаптуючись до нових викликів цифрової економіки. Ключовим завданням є забезпечення балансу між технологічними можливостями та необхідністю ефективного захисту прав учасників цивільного обороту [87, 123]. При цьому важливо зберегти фундаментальні принципи цивільно-правової відповідальності, адаптуючи їх до специфіки блокчейн-відносин.

Підсумовуючи, форми цивільно-правової відповідальності в блокчейн-відносинах мають свою специфіку застосування, зумовлену особливостями розподіленого реєстру та смарт-контрактів. Для ефективного використання різних форм відповідальності важливо забезпечити їх адаптацію до реалій блокчейн-середовища, зокрема, шляхом вироблення спеціальних підходів до визначення розміру відповідальності, забезпечення її фактичної реалізації, а також комбінування різних форм для оптимального захисту інтересів сторін. Вибір конкретної форми

відповідальності має ґрунтуватися на ретельному аналізі особливостей конкретних відносин та врахуванні технічних можливостей блокчейн-платформи.

Особливості підстав та форм відповідальності безпосередньо впливають на механізми розподілу ризиків між учасниками блокчейн-відносин.

Розподіл ризиків у блокчейн-середовищі базується на двох основних принципах: автономія учасників у прийнятті рішень щодо операцій та відповідальність за збереження власних криптографічних ключів [27, 91].

Розподіл ризиків здійснюється через:

1. Договірні механізми — прямий розподіл відповідальності в смарт-контрактах;
2. Технічні механізми — мультипідписні транзакції та порогові схеми;
3. Страхові механізми — децентралізовані протоколи страхування [67, 92].

Основним принципом розподілу ризиків у блокчейн-відносинах є те, що кожен учасник самостійно несе відповідальність за збереження своїх криптографічних ключів та безпеку своїх дій [14, 16]. Це відображає загальний принцип приватного права про автономію волі та відповідальність за власні рішення. Водночас технологічна складність та взаємозалежність учасників створюють ситуації, коли індивідуальні ризики можуть мати системний вплив.

У договірних відносинах розподіл ризиків зазвичай визначається умовами смарт-контракту або супровідного правочину. Сторони можуть передбачити, хто несе ризики збоїв, помилок у коді або зовнішніх факторів, що впливають на виконання зобов'язань [18, 36]. При цьому важливо враховувати, що деякі ризики, пов'язані з природою блокчейну, не можуть бути повністю виключені або перерозподілені.

Особливої уваги заслуговує питання форс-мажорних обставин у блокчейн-середовищі. Технічні збої, хакерські атаки або системні кризи можуть створювати ситуації, коли виконання зобов'язань стає неможливим або економічно недоцільним [20, 124]. У таких випадках важливо мати чіткі механізми визначення, чи є конкретна подія форс-мажором та як розподіляються ризики між сторонами.

Практика показує, що найбільш ефективним способом управління ризиками є їх попередня ідентифікація та розробка механізмів мінімізації. Це може включати

використання мультипідписів, страхування криптоактивів, створення резервних копій ключів та інші технічні та юридичні інструменти [37, 44]. При цьому важливо забезпечити баланс між безпекою та зручністю використання системи.

У відносинах з професійними учасниками (біржами, кастодіальними сервісами) розподіл ризиків часто визначається стандартними умовами надання послуг. Такі учасники зазвичай обмежують свою відповідальність, перекладаючи частину ризиків на користувачів [68, 109]. Це створює необхідність розробки механізмів розподілу ризиків, які б враховували як інтереси бізнесу, так і захист прав споживачів.

Таким чином, ефективний розподіл ризиків у блокчейн-середовищі вимагає комплексного підходу, що враховує як особливості, так і принципи справедливого розподілу відповідальності між учасниками приватно-правових відносин.

Проаналізувавши принципи розподілу ризиків, необхідно звернути увагу на проблематику обмеження відповідальності в блокчейн-середовищі.

В блокчейні застосовуються такі механізми обмеження відповідальності:

1. Кількісні обмеження розміру відповідальності;
2. Виключення відповідальності за певні категорії ризиків;
3. Встановлення умов звільнення від відповідальності [15, 103].

Аналіз практики обмеження відповідальності в блокчейн-середовищі виявляє дві основні моделі. Перша характерна для розробників платформ та смарт-контрактів, які прагнуть мінімізувати відповідальність за технічні помилки та непередбачені наслідки роботи коду [18, 36]. Друга модель притаманна централізованим сервісам (криптовалютним біржам, платіжним системам), де відповідальність обмежується кількісними показниками або вичерпним переліком випадків [67, 70].

Специфіка блокчейну зумовлює необхідність диференційованого підходу до встановлення меж відповідальності. Якщо для технологічних ризків виправданим є ширше обмеження відповідальності через об'єктивну складність прогнозування всіх сценаріїв роботи децентралізованої системи, то для випадків грубої недбалості або умисних порушень такі обмеження мають бути мінімальними.

Особливу теоретичну та практичну проблему становить обмеження відповідальності розробників смарт-контрактів. Концепція "код є законом" у блокчейні трансформує класичне розуміння меж відповідальності за програмні помилки [86, 91]. Проте повне звільнення розробників від відповідальності за наслідки автоматичного виконання смарт-контрактів суперечило б фундаментальним принципам цивільного права та створювало б невиправдані ризики для користувачів.

Механізми обмеження відповідальності мають корелювати з технічними можливостями відновлення прав. Незворотність блокчейн-транзакцій та відсутність централізованих механізмів примусового виконання зумовлюють необхідність формування альтернативної системи компенсаційних механізмів [26, 27]. Така система може включати спеціалізовані страхові фонди, децентралізовані механізми забезпечення виконання зобов'язань та багаторівневі гарантійні інструменти.

Імперативні обмеження відповідальності включають: заборону виключення відповідальності за умисні порушення; мінімальні стандарти захисту прав споживачів та обов'язкові вимоги до забезпечення безпеки операцій [99, 119].

Підсумовуючи, можна констатувати необхідність формування багаторівневої системи правового регулювання, яка б:

- Враховувала технологічну специфіку різних видів блокчейн-платформ;
- Диференціювала режими залежно від статусу учасників та характеру порушень;
- Забезпечувала ефективні механізми компенсації завданої шкоди;
- Встановлювала розумні межі договірного обмеження відповідальності.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. Проведений аналіз приватно-правового регулювання блокчейн-відносин демонструє трансформацію традиційних цивілістичних механізмів під впливом технологічних особливостей розподіленого реєстру. Це зумовлює необхідність адаптації класичних інститутів приватного права до специфіки цифрового середовища.

2. Аналіз загальних засад приватно-правового регулювання виявив унікальне поєднання диспозитивності з технологічною специфікою децентралізованих систем. Встановлено, що координаційний метод набуває нового змісту в умовах автоматизованого виконання зобов'язань, а принцип автономії волі трансформується через необхідність врахування технічних параметрів блокчейн-платформ.

3. Дослідження цивільно-правової природи блокчейн-правочинів розкрило особливості волевиявлення в цифровому середовищі та специфіку автоматизації виконання через смарт-контракти. Виявлено, що незмінність блокчейн-записів створює особливі вимоги до форми правочинів та механізмів реституції, а криптографічні методи стають невіддільною частиною процесу укладення договорів.

4. Аналіз договірних механізмів дозволив систематизувати основні види договорів з віртуальними активами та виявити специфіку забезпечення їх виконання. Встановлено, що традиційні способи забезпечення зобов'язань доповнюються новими формами, властивими блокчейн-середовищу, такими як мультипідписні транзакції та смарт-контракти з функцією умовного виконання.

5. Дослідження права власності на віртуальні активи виявило трансформацію класичної тріади правомочностей власника. Значення набуває взаємозв'язок між фактичним контролем над криптографічними ключами та юридичним титулом власності, що створює виклики для механізмів захисту та спадкування активів.

6. Аналіз цивільно-правового захисту в блокчейн-відносинах продемонстрував необхідність адаптації традиційних способів захисту до технічних особливостей розподіленого реєстру. Виявлено специфіку доказування, механізмів компенсації збитків та превентивних способів захисту в цифровому середовищі.

7. Дослідження інституту цивільно-правової відповідальності розкрило особливості підстав, форм та меж відповідальності в блокчейн-середовищі. Встановлено необхідність збалансованого розподілу ризиків між учасниками та розробки механізмів обмеження відповідальності з урахуванням специфіки децентралізованих систем.

8. На основі проведеного аналізу сформульовано ключові теоретичні положення щодо розвитку приватно-правового регулювання блокчейн-відносин. Необхідним є

забезпечення балансу між технологічною автоматизацією та правовою визначеністю, розробка спеціальних механізмів захисту прав учасників та формування єдиних підходів до регулювання нових видів договірних конструкцій.

Р О З Д І Л 3. Міжнародний досвід регулювання блокчейн-технологій

3.1. Міжнародний досвід та регуляторні підходи

У даному розділі проводиться порівняльно-правовий аналіз міжнародних підходів до регулювання блокчейн-технологій, що охоплює регуляторну практику провідних юрисдикцій, механізми гармонізації та захисту прав учасників, а також новітні підходи до регулювання інноваційних форм блокчейн-взаємодії.

Регулювання блокчейну пройшло еволюцію від загальних застережень центральних банків [108, 125], через формування спеціального законодавства [126] до комплексних регуляторних режимів [68, 112]. Регуляторна практика також трансформувалася від "м'яких" форм (рекомендації, роз'яснення) до обов'язкових нормативних вимог через закони та підзаконні акти [67, 99], зберігаючи при цьому експериментальні форми регулювання, такі як "пісочниці" та обмежені режими ліцензування.

Аналіз судової практики демонструє поступове формування правозастосовних підходів до блокчейн-технологій. Знаковою стала справа SEC v. Ripple Labs [41], де суд диференціював підхід до криптоактивів: інституційні продажі визнані інвестиційними контрактами, тоді як токени на вторинному ринку не кваліфіковано як цінні папери. У ЄС важливим прецедентом стало рішення у справі Skatteverket v. David Hedqvist [125], що звільнило обмін традиційних валют на біткоїн від ПДВ, визнавши його платіжним засобом .

Суттєвою характеристикою сучасного етапу є посилення ролі міжнародних організацій у формуванні стандартів регулювання [50, 99, 110]. Міжнародна група з протидії відмиванню коштів (далі також – "FATF") регулярно оновлює рекомендації щодо віртуальних активів та постачальників послуг щодо віртуальних активів (далі також – "VASP") [99]. Міжнародна організація зі стандартизації (далі також – "ISO") розробляє технічні стандарти для блокчейн-систем [50], а Міжнародна організація комісій з цінних паперів (далі також – "IOSCO") формує принципи регулювання бірж [67, 103]. Такі ініціативи створюють підґрунтя для гармонізації національних підходів, хоча й зберігаються суттєві відмінності в їх імплементації.

Аналіз міжнародного досвіду дозволяє виділити декілька ключових трендів у розвитку регулювання блокчейн-технологій на сучасному етапі; перехід від фрагментарного до системного регулювання, що охоплює всі аспекти блокчейн-екосистеми; диференціація регуляторних вимог залежно від типу криптоактивів та ризиків, які вони створюють; посилення вимог до захисту прав споживачів та інвесторів при збереженні простору для інновацій; розвиток механізмів міжнародної координації та гармонізації регуляторних підходів та адаптація регулювання до нових форм блокчейн-взаємодії (DeFi, DAO, NFT).

Ці тренди формують рамки для аналізу конкретних регуляторних моделей різних юрисдикцій, що розглядаються далі.

Регуляторний підхід ЄС базується на MiCA [68], який встановлює три основні категорії токенів: токени, прив'язані до активів, токени електронних грошей та інші.

Для кожної категорії токенів встановлено диференційовані вимоги щодо емісії, обігу та розкриття інформації. Особливої уваги заслуговує режим для "значних" токенів (прив'язаних до активів та електронних грошей), які можуть мати системний вплив на фінансову стабільність. Такі токени підлягають підвищеним вимогам щодо капіталу, резервів, ліквідності та корпоративного управління, а також можуть підпадати під прямий нагляд з боку Європейського банківського органу [68].

MiCA також детально регламентує діяльність VASP, класифікуючи їх за основними типами послуг: зберігання та адміністрування криптоактивів, торгові операції, обмінні послуги, виконання ордерів та консультування.

Для здійснення діяльності в ЄС такі провайдери мають отримати ліцензію від національного регулятора та дотримуватися вимог щодо капіталу, корпоративного управління, розділення активів клієнтів, захисту прав споживачів та інформаційної безпеки. MiCA запроваджує принцип єдиного європейського паспорта, що дозволяє CASP надавати послуги в усіх державах-членах ЄС без додаткових дозволів [68].

Важливим аспектом регулювання є також встановлення єдиних правил запобігання ринковим зловживанням, зокрема маніпулюванню цінами та інсайдерській торгівлі. MiCA вводить заборону на поширення недостовірної

інформації, маніпулятивні транзакції та інші форми недобросовісної поведінки на ринку криптоактивів, що значно підвищує рівень захисту інвесторів [68].

Слід зазначити, що MiCA не регулює криптоактиви, які вже підпадають під дію чинного фінансового законодавства, зокрема токенізовані цінні папери та інші фінансові інструменти. Такі активи продовжують регулюватися відповідно до Директиви про ринки фінансових інструментів та інших відповідних актів [15].

Важливим доповненням до MiCA є DLT Pilot Regime [19], що створює регуляторну "пісочницю" для тестування інфраструктур, які використовують блокчейн для фінансових інструментів. Також регламент eIDAS 2.0 передбачає використання децентралізованих ідентифікаторів у єдиній системі цифрової ідентичності ЄС, розширюючи застосування блокчейну у публічному секторі [14].

Водночас залишається відкритим питання гармонізації вимог GDPR з технологією блокчейну. Регулятори наголошують на необхідності впровадження механізмів "privacy by design", таких як використання зовнішніх сховищ персональних даних та застосування криптографічних інструментів конфіденційності [15, 26]. Французький регулятор CNIL випустив у 2018 році детальні рекомендації щодо застосування GDPR у блокчейн-проєктах, де запропонував технічні рішення для забезпечення права на видалення даних через мінімізацію обсягу інформації в блокчейні та використання техніки "хешування з секретом" [38].

Окрему увагу ЄС приділяє потенціалу блокчейну в модернізації фінансового сектору. Європейський центральний банк активно досліджує можливості випуску CBDC на базі інфраструктури блокчейну [52]. У жовтні 2021 року ЄЦБ розпочав дворічну дослідницьку фазу проєкту, а у 2023 році перейшов до тестування прототипів цифрового євро. Хоча цифровий євро не позиціюється як криптовалюта, його архітектура може включати окремі елементи блокчейну, адаптовані під централізований контроль. Це демонструє інтерес до технології з боку традиційних фінансових інститутів, які прагнуть підвищити ефективність і безпеку розрахунків.

Порівнюючи підхід ЄС з іншими юрисдикціями, можна відзначити його більш структурований і деталізований характер. На відміну від США, де переважає точковий підхід, заснований на тлумаченні чинного законодавства про цінні папери

та товарні деривативи, ЄС через MiCA запроваджує спеціалізований режим для всього спектру криптоактивів. При цьому ЄС, як і США, приділяє значну увагу захисту прав інвесторів і споживачів, встановлюючи підвищені вимоги до розкриття інформації та запобігання маніпуляціям [26]. Водночас європейська модель передбачає більший акцент на уніфікації правил у рамках єдиного ринку, тоді як у США зберігається суттєва роль розрізненого регулювання на рівні штатів.

Порівняно з азійськими юрисдикціями, такими як Японія та Сінгапур, підхід ЄС характеризується більшою збалансованістю між стимулюванням інновацій та жорсткістю регуляторних вимог. З одного боку, MiCA створює правову визначеність для учасників ринку, з іншого – встановлює чіткі запобіжники для мінімізації ризиків [119]. Однак азійські країни історично демонструють більшу гнучкість і оперативність в адаптації законодавства до потреб блокчейн-індустрії, зокрема через впровадження "регуляторних пісочниць" [67].

Імплементація MiCA відбувається поетапно: більшість положень стосовно емітентів стейблкоїнів набули чинності у червні 2023 року, а вимоги до VASP застосовуються з грудня 2024 року.

Регуляторна модель ЄС вирізняється комплексністю та прагненням забезпечити визначеність через структуровану класифікацію токенів, детальні правила діяльності провайдерів та адаптацію суміжних сфер регулювання до специфіки блокчейну.

Правове регулювання блокчейн-технологій у США має багаторівневу структуру з розподілом компетенції між федеральними та штатними органами. На національному рівні SEC тлумачить більшість інвестиційно привабливих токенів, включаючи утилітарні, як цінні папери згідно з "тестом Хоуї", що вимагає дотримання вимог щодо реєстрації випуску та розкриття інформації [17, 41, 67].

Іншим важливим гравцем є Комісія з торгівлі товарними ф'ючерсами (далі також – "CFTC"), яка розглядає деякі криптовалюти (біткоїн) як товар [103]. Це надає CFTC юрисдикцію щодо криптодеривативів та вимагає від криптобірж реєструватись як торгові платформи. У кількох справах [129, 130] CFTC застосовувала законодавство про товарні деривативи для притягнення до відповідальності криптовалютні

платформи, які порушували вимоги до реєстрації або маніпулювали ринком [125, 128].

Судова практика США формує важливі прецеденти, зокрема у справах SEC v. Ripple Labs [41], де був застосований диференційований підхід до токенів залежно від контексту їх продажу, та CFTC v. Ooki DAO [129], що встановила відповідальність членів DAO за прийняті колективні рішення. Ці рішення демонструють еволюцію від спрощеного розуміння криптоактивів до нюансованих підходів, що враховують специфіку різних форм блокчейн-відносин.

Паралельно Мережа боротьби з фінансовими злочинами (FinCEN) встановлює правила протидії відмиванню коштів для криптовалютних бірж та інших VASP [103]. Згідно з рекомендаціями FinCEN, такі суб'єкти мають реєструватись як установи, що надають грошові послуги, та впроваджувати процедури KYC. Недотримання цих вимог загрожує суттєвими санкціями з боку регулятора [113].

На відміну від єдиного європейського MiCA, американське законодавство не містить окремого акту про криптоактиви. Натомість регулювання здійснюється через тлумачення наявних норм про цінні папери, товарні деривативи та AML [67]. Це створює певну фрагментарність і непередбачуваність регуляторного середовища, особливо щодо проєктів, які не підпадають під традиційні категорії.

У Конгресі США розглядаються ініціативи щодо створення спеціалізованих режимів для окремих видів криптоактивів. На рівні штатів спостерігається різноманіття підходів: від досить ліберального режиму в Вайомінгу, який визнає токени самостійним видом активів, до жорсткіших правил у Нью-Йорку, де діє спеціальний дозвіл BitLicense для бізнесу [66, 131]. Така неоднорідність створює виклики для компаній, що здійснюють діяльність.

Вайомінг демонструє прогресивний підхід, створивши комплексну правову базу для розвитку блокчейн-індустрії, включаючи спеціальний Wyoming DAO LLC Act [66], що регулює DAO (детальніше розглянуто в підрозділі 3.2). Інший важливий акт – Wyoming Special Purpose Depository Institution (SPDI) Act, що дозволяє створювати спеціалізовані банки для обслуговування криптовалютних компаній [66].

На противагу цьому, Нью-Йорк запровадив BitLicense – один із найбільш жорстких регуляторних режимів для криптобізнесу. Департамент фінансових послуг Нью-Йорка встановлює високі вимоги до капіталу, комплаєнсу, кібербезпеки та корпоративного управління [131]. Це призвело до обмеженої кількості ліцензованих компаній і критики з боку індустрії щодо надмірних регуляторних бар'єрів.

Порівнюючи американську модель із підходами інших юрисдикцій, можна зазначити, що США активно застосовують наявне законодавство до криптосектору, тоді як ЄС та азійські країни частіше вдаються до прийняття спеціальних норм. Американські регулятори, зокрема SEC, схильні трактувати більшість інвестиційних токенів як цінні папери, що приваблює інвесторів, але створює бар'єри для входу на ринок [47]. Водночас окремі штати, такі як Вайомінг, пропонують альтернативні моделі регулювання, орієнтовані на стимулювання блокчейн-інновацій [66].

США також беруть активну участь у міжнародній координації регулювання криптоактивів. Американські регулятори співпрацюють з FATF щодо впровадження стандартів протидії відмиванню коштів та "правила подорожі", а також з Радою з фінансової стабільності (далі також – "FSB") та G20 щодо розробки глобальних принципів регулювання [67, 99]. Ця діяльність демонструє прагнення США впливати на формування міжнародних стандартів та запобігати регуляторному арбітражу.

Американська модель характеризується поєднанням жорстких вимог федеральних агентств із регуляторним різноманіттям на рівні штатів. Попри відсутність єдиного закону про криптоактиви, США демонструють послідовність у захисті прав інвесторів. Значний вплив США на міжнародну фінансову систему зумовлює потенціал екстериторіального застосування американських підходів, що матиме наслідки для глобальної блокчейн-індустрії.

Регуляторні підходи в Азії демонструють широкий діапазон позицій: від майже повної заборони до створення сприятливих "регуляторних пісочниць" для блокчейн-проєктів [67]. Ключовими гравцями регіону є Китай, Японія, Сінгапур та Південна Корея, кожен з яких пропонує особливу модель взаємодії з криптоіндустрією.

Китай історично посідає унікальне місце, поєднуючи активну підтримку блокчейн-інновацій на державному рівні з жорсткими обмеженнями на

децентралізовані криптовалюти [103]. З 2017 року Народний банк Китаю послідовно впроваджував заборони на ICO та діяльність криптовалютних бірж, аргументуючи це ризиками для фінансової стабільності та контролю за капіталом [103]. У 2021 році обмеження суттєво посилилися після видання Повідомлення Народного банку Китаю про заборону всіх операцій з криптовалютами, що фактично криміналізувало будь-яку діяльність, пов'язану з торгівлею та обміном криптовалют [70]. Незабаром після цього обмеження поширилися на майнінг криптовалют, що призвело до масштабної міграції майнінгових потужностей до інших країн [53].

Водночас Китай активно розвиває власну інфраструктуру CBDC на базі керованої версії блокчейну [16]. Проєкт цифрового юаня демонструє прагнення Китаю використовувати переваги блокчейн-технологій під централізованим наглядом держави [52]. На відміну від класичних криптовалют, цифровий юань повністю контролюється Народним банком Китаю, який може відстежувати всі транзакції та за необхідності блокувати окремі рахунки [98]. Така модель контрастує з ідеологією криптовалют, заснованих на децентралізації та анонімності транзакцій.

Азійські юрисдикції демонструють різноманітні підходи до регулювання криптоактивів. Японія впровадила чітку систему ліцензування через поправки до Закону про платіжні послуги, визнавши криптовалюти легальним засобом платежу [132]. Особливістю японської моделі є значна роль саморегулювання через Японську асоціацію бірж цифрових активів, що розробляє галузеві стандарти.

Сінгапур позиціює себе як глобальний хаб для блокчейн-інновацій, запровадивши Закон про платіжні послуги та використовуючи "регуляторні пісочниці" для експериментів під наглядом Валютного управління Сінгапуру (далі також – "MAS") [119]. Програма Fintech Regulatory Sandbox дозволяє проєктам тестувати рішення в середовищі з доступом до спрощених вимог [19].

Південна Корея демонструє збалансований підхід, запровадивши у 2021 році Закон про звітність та використання спеціальної фінансової інформації з жорсткими вимогами до KYC через банківські рахунки та інтеграцію криптоактивів у податкову систему зі ставкою 20% для прибутків понад 2,5 млн вон на рік [107].

Порівнюючи азійські підходи між собою та з іншими регіонами, можна зазначити, що в Азії спостерігається більша поляризація регуляторних моделей [67]. Якщо Китай робить ставку на державний контроль та власні цифрові валюти, то Японія та Сінгапур прагнуть інтегрувати криптоіндустрію в правове поле через ліцензування та цільові нормативні режими [132]. Порівняно зі США та ЄС, азійські юрисдикції часто демонструють більшу гнучкість і готовність до експериментів, особливо в аспекті впровадження блокчейну в публічному секторі [67].

Перспективи регулювання в Азії багато в чому залежатимуть від здатності країн знайти баланс між інноваціями та стабільністю. Для Китаю ключовим викликом буде гармонізація цифрового юаня з міжнародними стандартами та забезпечення його сумісності з іншими платіжними системами [52]. Японія та Сінгапур, своєю чергою, мають потенціал стати регіональними центрами компетенцій у сфері блокчейну, задаючи тон у розробці технічних і правових рішень [113].

Корея, з її збалансованим підходом, демонструє модель, що може бути привабливою для країн, які прагнуть поєднати інновації з надійним захистом споживачів. Особливий інтерес становить корейський досвід інтеграції криптоактивів у банківську систему через прив'язку до рахунків на реальні імена, що забезпечує високий рівень прозорості без надмірних обмежень на розвиток галузі [107].

Загалом, азійський досвід демонструє, що регулювання блокчейн-технологій може набувати різних форм залежно від національних пріоритетів та соціально-економічних умов. Попри відмінності в підходах, спільною тенденцією для країн регіону є визнання трансформаційного потенціалу блокчейну та пошук оптимальних моделей його інтеграції в державну політику та правову систему.

Окрему категорію юрисдикцій складають країни, які формують сприятливе середовище для залучення бізнесу [67]. Серед них особливе місце посідають Швейцарія, Мальта, Ліхтенштейн та Об'єднані Арабські Емірати (далі також – "ОАЕ"), чиї підходи стали своєрідним еталоном для багатьох учасників індустрії.

Швейцарія однією з перших запропонувала чітку класифікацію токенів, розмежовуючи платіжні, утилітарні та цінні (security) токени [67]. Швейцарське Управління з нагляду за фінансовими ринками оцінює кожен проєкт індивідуально,

застосовуючи функціональний підхід: якщо токен має ознаки цінного паперу, до нього застосовуються вимоги щодо реєстрації випуску та розкриття інформації. Водночас утилітарні токени, які надають доступ до продуктів або послуг, підлягають м'якшим вимогам [60]. Такий підхід забезпечує гнучкість регулювання та дозволяє блокчейн-компаніям обирати оптимальну модель токенізації.

Особливе значення для розвитку швейцарського блокчейн-регулювання мало прийняття Федерального закону про адаптацію федерального законодавства до розвитку технології розподіленого реєстру (DLT Act) [113]. Цей акт здійснив оновлення швейцарського цивільного та фінансового законодавства для створення умов для розвитку блокчейн-технологій та токенізованої економіки. Ключовою інновацією стало впровадження концепції "реєстрованих цінних прав", які можуть випускатись і обертатися у формі токенів на блокчейні [113]. Закон визначає вимоги до блокчейн-реєстрів, які можуть використовуватися для фіксації таких прав, а також правові наслідки передачі токенів, що представляють ці права [93].

DLT Act також запровадив спеціальну категорію ліцензій для "DLT-торгових систем", що дозволяють здійснювати організовану торгівлю токенізованими цінними паперами [113]. Такі системи можуть надавати послуги не лише професійним учасникам ринку, але й роздрібним інвесторам, що відрізняє їх від традиційних біржових систем. При цьому до них застосовуються адаптовані вимоги щодо захисту інвесторів, управління ризиками та протидії маніпулюванню ринком.

Іншим важливим фактором привабливості Швейцарії стало створення так званої "Криптодолини" у кантоні Цуг [113]. Ця ініціатива об'єднує блокчейн-стартапи, дослідницькі центри та інвесторів, пропонуючи їм сприятливий податковий режим і доступ до кадрів. Наявність такої екосистеми сприяє розвитку інноваційних проєктів і посилює позиції Швейцарії як глобального блокчейн-хабу [19].

Мальта, своєю чергою, позиціює себе як "Острів блокчейну", пропонуючи комплексну законодавчу базу для криптоіндустрії. Ключовими елементами мальтійського регулювання є Закон про віртуальні фінансові активи (VFA Act), Закон про інноваційні технологічні послуги (ITAS Act) та Закон про цифрові інноваційні

авторитети (MDIA Act). Ця тріада актів встановлює правила випуску токенів, ліцензування криптовалютних сервісів, а також принципи захисту інвесторів [67].

Особливістю мальтійського підходу є впровадження обов'язкового тесту фінансових інструментів (Financial Instrument Test), який дозволяє визначити природу токена та застосовні до нього вимоги. Методологія цього тесту передбачає послідовний аналіз характеристик токена на основі запитальника, розробленого Мальтійським органом з фінансових послуг. Залежно від результатів тесту, токен може кваліфікуватися як віртуальний токен, фінансовий інструмент, електронні гроші або віртуальний фінансовий актив. Кожна категорія має специфічні правила випуску та обігу, а також вимоги до емітентів і провайдерів послуг [51].

Закон про інноваційні технологічні послуги (ITAS Act) додатково запроваджує режим для технологічних провайдерів, які надають послуги з розробки, впровадження та аудиту DLT-систем [67]. Це дозволяє забезпечити якість та надійність технологічної інфраструктури, на основі якої функціонують блокчейн-проєкти. Запровадження такого режиму демонструє комплексний підхід Мальти, що охоплює не лише фінансові, але й технологічні аспекти регулювання.

Ліхтенштейн, розробив один із найбільш інноваційних підходів до регулювання блокчейн-технологій. У 2020 році тут набув чинності Закон про токени та надійних постачальників технологічних послуг (TVTG, також відомий як Blockchain Act) [112]. Цей закон пропонує унікальну концепцію "токена як контейнера", в якому можуть міститися різні права – від права власності на фізичні активи до прав вимоги, авторських прав чи членських прав у юридичних особах. Такий підхід дозволяє токенізувати будь-які види активів у рамках єдиної правової парадигми.

TVTG запроваджує десять категорій "постачальників послуг ТТ", включаючи генераторів токенів, зберігачів приватних ключів, верифікаторів токенів, провайдерів фізичних валідаторів та інших [112]. Для кожної категорії встановлюються вимоги щодо реєстрації, капіталу, корпоративного управління та дотримання правил AML/CFT [133]. Особливістю Ліхтенштейну є технологічна нейтральність – закон не обмежується технологіями, а створює умови для систем розподіленого реєстру [37].

Закон також вводить поняття "системи ТТ" (системи довірених технологій), що охоплює будь-які блокчейн-платформи та інші розподілені реєстри [112]. Це значно розширює сферу застосування акту порівняно з іншими юрисдикціями, які часто обмежуються регулюванням лише криптоактивів. Такий комплексний підхід створює правову визначеність для широкого спектра блокчейн-застосунків – від цифрових валют до систем управління ланцюгами постачання [133].

ОАЕ демонструють комплексний підхід до розвитку блокчейн-екосистеми через кілька ключових ініціатив: Emirates Blockchain Strategy 2021 для цифровізації державних послуг, створення спеціалізованого регуляторного органу Dubai Virtual Assets Regulatory Authority (VARA) із поступовим розширенням дозволених активів за моделлю "мінімального життєздатного продукту", та спеціальні ліцензійні режими в економічних зонах, зокрема DMCC [19]. Цей підхід поєднує стимулювання інновацій із забезпеченням належного регуляторного нагляду [61].

Підхід Швейцарії, Мальти, Ліхтенштейну та ОАЕ відрізняється від США та ЄС створенням спеціалізованих правових режимів для блокчейн-індустрії при збереженні стандартів захисту інвесторів [113].

Досвід цих країн демонструє, що продумана регуляторна стратегія здатна перетворити країну на впливового гравця на криптовалютному ринку. Поєднання правової визначеності, гнучкості вимог та сприятливого бізнес-клімату приваблює блокчейн-підприємців з усього світу, стимулюючи інновації та економічне зростання.

Модель "криптодолин" та інноваційних регуляторних зон породжує виклики, пов'язані з управлінням ризиками та запобіганням регуляторному арбітражу. Щоб запобігти використанню ліберальних режимів для незаконних практик, варто забезпечувати моніторинг і співпрацю з міжнародними органами [122].

Загалом, Швейцарія, Мальта, Ліхтенштейн та ОАЕ пропонують унікальні підходи до регулювання блокчейн-технологій, які поєднують інноваційність з відповідальністю. Їхній досвід може слугувати орієнтиром для інших юрисдикцій, які прагнуть створити збалансовану та ефективну регуляторну екосистему для розвитку блокчейн-індустрії. При цьому важливо враховувати національну специфіку та

забезпечувати синхронізацію з глобальними ініціативами щодо стандартизації та міжнародної співпраці у сфері регулювання блокчейну.

Порівняльний аналіз ускладнюється термінологічними розбіжностями між юрисдикціями ("віртуальні активи", "криптоактиви", "цифрові платіжні токени"), але дозволяє виявити закономірності та сформувати типологію регуляторних моделей для прогнозування їх розвитку та ефективності.

Аналіз міжнародного досвіду виявляє три основні типи регуляторних підходів: відкрито-ліберальні (Швейцарія, Сінгапур, Японія, Ліхтенштейн, ОАЕ), що створюють правові режими для блокчейн-проєктів при збереженні захисту інвесторів; помірковано-регульовані (США, ЄС, Південна Корея), що адаптують традиційне законодавство до криптоактивів; та жорстко-рестриктивні (Китай), що обмежують криптовалюти на користь державних CBDC [16, 67, 103].

Ефективність регуляторних моделей можна оцінювати за кількома ключовими параметрами: підходом до втручання (проактивний, реактивний, експериментальний), методом класифікації криптоактивів (функціональний, ризик-орієнтований, інтеграційний) та рівнем технологічної нейтральності регулювання. Ця класифікація дозволяє точніше позиціювати регуляторні режими різних країн.

Запропонована типологія відображає основні регуляторні стратегії, хоча в межах кожного типу існують варіації та експериментальні режими. Для їх систематизації доцільно застосувати теоретичні концепції "ризик-орієнтованого регулювання" Дж. Блека та регуляторної конкуренції Д. Мерфі [134], аналізуючи регуляторні моделі за параметрами: спрямованості на ризики чи можливості, проактивності чи реактивності втручання, формальності чи гнучкості механізмів [135].

Важливим фактором збалансованості є міжнародна координація та гармонізація підходів для мінімізації ризиків регуляторного арбітражу. Ключову роль тут відіграють міжнародні організації (FATF, IOSCO), що формують рекомендації щодо уніфікації процедур ліцензування, ідентифікації клієнтів та розкриття інформації, а також регіональні ініціативи, як-от MiCA в ЄС.

Вибір оптимальної моделі регулювання вимагає балансу між стимулюванням інновацій та забезпеченням стабільності й захисту прав. Досягнення цього балансу

можливе лише за умови активного діалогу між регуляторами, індустрією та громадянським суспільством, а також міжнародної співпраці для створення адаптивної системи регулювання, що відповідає потребам цифрової економіки.

Підсумовуючи, аналіз міжнародного досвіду демонструє необхідність адаптивного та збалансованого регулювання, яке стимулює інновації, забезпечуючи при цьому стабільність та захист прав. Розглянемо детальніше роль міжнародних організацій у формуванні глобальних стандартів регулювання блокчейн-технологій.

Попри відмінності у підходах до регулювання блокчейн-технологій, спостерігається тенденція до їх гармонізації, де ключову роль відіграють міжнародні організації, що формують стандарти та рекомендації [99, 50]. Особливе значення має діяльність FATF у формуванні стандартів AML/CFT щодо віртуальних активів, а технічна стандартизація здійснюється в рамках ISO/TC 307, який розробляє стандарти з термінології, безпеки, сумісності та управління блокчейн-системами [50, 95, 96].

WIPO активно досліджує можливості використання блокчейну для захисту прав інтелектуальної власності [136]. Організація розробляє рекомендації щодо використання технології для реєстрації прав, управління ліцензіями та захисту від порушень. Особлива увага приділяється питанням транскордонного визнання блокчейн-записів як доказів права інтелектуальної власності [117].

Світовий банк та МВФ також беруть участь у формуванні підходів до регулювання блокчейн-технологій, зокрема в контексті CBDC та модернізації фінансової інфраструктури [52, 113]. Їхні дослідження та рекомендації впливають на формування політик щодо впровадження блокчейну у фінансовому секторі.

ОЕСР працює над виробленням єдиних підходів до оподаткування операцій з віртуальними активами [19]. Розроблений організацією Common Reporting Standard поступово адаптується для охоплення операцій з криптоактивами, що має сприяти підвищенню прозорості та протидії ухиленню від оподаткування [94].

Системний аналіз діяльності міжнародних організацій у сфері регулювання блокчейн-технологій дозволяє зробити наступні висновки.

По-перше, міжнародні організації відіграють роль у формуванні підходів, створюючи стандарти "м'якого права", які імплементуються в національне право.

По-друге, спостерігається чітка спеціалізація міжнародних організацій: FATF фокусується на протидії відмиванню коштів, ISO — на технічній стандартизації, Всесвітня організація інтелектуальної власності (далі також – "WIPO") — на захисті інтелектуальної власності, що забезпечує комплексний підхід до регулювання.

По-третє, імплементація стандартів відрізняється залежно від юрисдикції, що створює ризики регуляторного арбітражу та ускладнює транскордонний нагляд [67].

По-четверте, сфера діяльності міжнародних організацій розширюється від криптовалют до нових форм блокчейн-відносин, таких як DeFi, NFT та DAO [18].

По-п'яте, зростає роль механізмів координації між міжнародними організаціями для забезпечення узгодженості підходів та уникнення дублювання вимог [50].

У контексті міжнародної гармонізації ключову роль відіграє імплементація стандартів FATF щодо віртуальних активів та VASP у національних юрисдикціях, зокрема впровадження "правила подорожі" для транскордонних транзакцій [99].

Оцінки FATF демонструють різний рівень імплементації "правила подорожі". Швейцарія впровадила вимоги через Self-Regulatory Organization та Закон про боротьбу з відмиванням грошей [136], а Сінгапур інтегрував їх у Закон про платіжні послуги з диференційованим підходом залежно від типу VASP та ризиків [113].

Водночас практичне впровадження "правила подорожі" стикається з технічними та організаційними викликами. Основні проблеми включають:

- Відсутність стандартизованих протоколів обміну інформацією між VASP;
- Складність верифікації даних, отриманих від інших провайдерів;
- Забезпечення конфіденційності переданої інформації;
- Застосування правила до платформ без центрального оператора [47].

Індустрія розробляє технічні рішення для розв'язання цих проблем. Ініціативи, такі як Travel Rule Information Sharing Alliance (TRISA), OpenVASP, Travel Rule Protocol (TRP) та InterVASP Messaging Standard (IVMS101), спрямовані на створення стандартизованих протоколів для обміну інформацією відповідно до вимог FATF. Ці рішення використовують різні підходи – від централізованих систем обміну до децентралізованих протоколів на базі блокчейну [99].

Особлива увага приділяється вимогам щодо належної перевірки клієнтів (KYC). FATF наголошує на необхідності ідентифікації не лише безпосередніх клієнтів VASP, але й кінцевих бенефіціарів операцій. Це вимагає впровадження складних систем верифікації та моніторингу, особливо у випадках використання анонімних криптовалют або змішувачів (mixers) [101, 113].

Регулярні оцінки FATF демонструють значний прогрес у впровадженні рекомендацій на національному рівні. Станом на 2025 рік більшість розвинених країн адаптували своє законодавство відповідно до вимог FATF щодо регулювання віртуальних активів. Водночас зберігаються суттєві відмінності в підходах до імплементації цих вимог, що створює ризики регуляторного арбітражу [47, 113].

Азійські юрисдикції демонструють різні шляхи імплементації міжнародних стандартів: Японія впровадила комплексну систему AML/CFT з жорсткими вимогами до VASP через Закон про платіжні послуги, забезпечуючи високий рівень відповідності глобальним стандартам при збереженні національної специфіки правозастосування [137]. Сінгапур застосовує диференційований ризик-орієнтований підхід, де рівень контролю визначається аналізом бізнес-моделі, клієнтської бази та інфраструктури VASP, що забезпечує пропорційність регулювання [113].

Ефективність рекомендацій FATF значною мірою залежить від спроможності забезпечити їх виконання в децентралізованому середовищі. Особливо складним є питання регулювання DeFi-протоколів, де часто відсутній чітко визначений оператор, який міг би виконувати функції VASP. Це вимагає розробки нових підходів до регулювання, що враховували б специфіку децентралізованих систем [91, 96].

Критики підходу FATF вказують на потенційні ризики надмірного регулювання, яке може підірвати інноваційний потенціал блокчейн-технологій та призвести до витіснення легальної активності в нерегульований сектор. Водночас практика показує, що чіткі регуляторні вимоги сприяють інституціоналізації індустрії та підвищенню довіри з боку традиційного фінансового сектору [14, 67].

Створений у 2016 році технічний комітет ISO/TC 307 розробляє міжнародні стандарти для блокчейн-технологій, забезпечуючи інтероперабельність та безпеку систем через єдині технічні специфікації [50].

Основними напрямами стандартизації є термінологія, архітектура та таксономія блокчейн-систем, безпека та конфіденційність, смарт-контракти, управління та взаємодія різних блокчейн-мереж. Особлива увага приділяється розробці стандартів щодо функціональної сумісності різних блокчейн-платформ, що має критичне значення для розвитку глобальної блокчейн-інфраструктури [2, 50].

ISO розробив комплекс стандартів для блокчейн-технологій: ISO 22739:2020 встановлює єдину термінологію, ISO/TR 23455:2019 визначає принципи функціонування смарт-контрактів, а ISO/TR 23576:2020 регламентує вимоги до безпеки зберігання активів. Ці стандарти створюють підґрунтя для розробки регуляторних норм, сприяючи гармонізації підходів на міжнародному рівні.

Важливим аспектом діяльності ISO є розробка стандартів безпеки для блокчейн-систем. Комітет працює над визначенням вимог до криптографічних механізмів, процедур управління ключами, захисту персональних даних та забезпечення цілісності даних. Ці стандарти створюють технічну основу для впровадження регуляторних вимог щодо захисту прав учасників [95, 96].

У сфері смарт-контрактів ISO розробляє стандарти, що визначають архітектуру, принципи безпеки та механізми взаємодії. Ці стандарти мають особливе значення для розвитку правового регулювання автоматизованого виконання договорів, оскільки створюють технічну базу для оцінки надійності та безпеки смарт-контрактів [26, 79].

Хоча стандарти ISO не мають юридичної сили, вони активно використовуються при розробці національного законодавства та формуванні регуляторних вимог. Багато країн інкорпорують технічні вимоги ISO у свої нормативні акти, що сприяє гармонізації технічних аспектів регулювання блокчейн-технологій [39, 113].

Швейцарія, наприклад, активно впроваджує стандарти ISO при розробці технічних вимог до блокчейн-систем, що використовуються для створення "реєстрованих цінних прав" відповідно до Федерального закону про адаптацію федерального законодавства до розвитку технології розподіленого реєстру (DLT Act). Технічні вимоги до таких систем, зокрема щодо цілісності даних, доступності та захисту від несанкціонованого доступу, базуються на стандартах ISO/TC 307 [113].

Сінгапур також використовує стандарти ISO у своїй практиці. MAS розробило вимоги до інфраструктури VASP на основі рекомендацій ISO/TC 307, зокрема щодо управління ключами, безпеки зберігання активів та захисту від кібератак [138].

Процес імплементації стандартів ISO супроводжується викликами, зокрема через розвиток технологій та появу нових форм блокчейн-взаємодії. Це вимагає оновлення стандартів та забезпечення їх актуальності [91, 96].

Іншим викликом є забезпечення балансу між точністю стандартів та їх зрозумілістю для регуляторів і законодавців, які часто не мають глибоких технічних знань. Для подолання цього розриву ISO/TC 307 співпрацює з іншими міжнародними організаціями, такими як FATF, IOSCO та Світовий банк, з метою розробки керівних принципів щодо застосування технічних стандартів у регуляторній практиці [39].

Важливо відзначити, що стандарти ISO створюють не лише технічне, але й термінологічне підґрунтя для розвитку правових механізмів. Єдина термінологія, закріплена у стандарті ISO 22739:2020, поступово імплементується в національне законодавство різних країн, сприяючи формуванню спільного понятєвого апарату та полегшуючи транскордонну взаємодію [21]. Це забезпечує тісний зв'язок між технічними стандартами та правовими механізмами захисту прав учасників, які розглядаються у підрозділі 3.2. Так, технічні вимоги до смарт-контрактів, закріплені в ISO/TR 23455:2019, закладають основу для правової кваліфікації автоматизованого виконання зобов'язань та визначення відповідальності за помилки в коді.

WIPO відіграє провідну роль у формуванні міжнародних підходів до захисту прав інтелектуальної власності в контексті блокчейн-технологій. Організація активно досліджує потенціал використання блокчейну для вдосконалення систем реєстрації та захисту прав інтелектуальної власності [136].

Основна увага WIPO зосереджена на дослідженні можливостей блокчейну для управління правами інтелектуальної власності. Організація розглядає технологію як інструмент для забезпечення прозорості та достовірності інформації про права інтелектуальної власності, автоматизації процесів та розподілу роялті [80, 105].

У своїй Білій книзі "WIPO Blockchain White Paper" організація окреслює перспективи створення блокчейн-реєстрів для різних об'єктів інтелектуальної

власності. Це могло б забезпечити миттєву верифікацію прав, відстеження використання творів та розподіл винагороди між правовласниками [136, 143].

Особлива увага приділяється питанням захисту авторських прав. WIPO досліджує можливості використання блокчейну для боротьби з піратством, забезпечення винагороди авторам та спрощення процедур ліцензування [111].

Практичною реалізацією цих досліджень став проєкт WIPO PROOF, який використовує технологію блокчейн для створення цифрових доказів існування та володіння інтелектуальною власністю. Сервіс дозволяє авторам та винахідникам створювати цифрові відбитки (хеші) своїх творів та зберігати їх у захищеному реєстрі з часовою міткою [136]. Це забезпечує доказову базу для підтвердження першості створення та допомагає вирішувати спори щодо авторства.

WIPO також співпрацює з Creative Commons та іншими організаціями щодо розробки блокчейн-рішень для управління авторськими правами. Одним із напрямів такої співпраці є створення стандартизованих метаданих для творів, що дозволяють автоматично відстежувати їх використання та забезпечувати справедливу винагороду авторам. Такі системи особливо важливі для музичної індустрії, де складні ланцюжки прав та роялті часто призводять до затримок виплат та суперечок [120, 136].

WIPO також розглядає потенціал блокчейну для модернізації патентної системи. Технологія може забезпечити більш ефективну перевірку новизни винаходів, автоматизувати процеси реєстрації та ліцензування патентів, а також спростити міжнародну взаємодію патентних відомств [73, 117].

Значна увага приділяється розробці механізмів вирішення спорів щодо інтелектуальної власності з використанням блокчейн-технологій. WIPO досліджує можливості створення децентралізованих систем арбітражу та медіації, які могли б забезпечити швидке та ефективне врегулювання конфліктів [25, 136].

Однак впровадження рекомендацій WIPO стикається з викликами, зокрема щодо забезпечення сумісності різних систем реєстрації прав, захисту конфіденційної інформації та визначення юридичної сили записів у різних юрисдикціях [95, 111].

Окремою проблемою є питання захисту прав інтелектуальної власності на NFT. WIPO розробляє рекомендації щодо розмежування прав на токен та базовий актив,

визначення обсягу прав, що передаються при продажу NFT, та механізмів захисту авторів від несанкціонованої токенізації їхніх творів. Ці рекомендації можуть стати основою для гармонізації національних підходів до регулювання ринку NFT [73].

WIPO також приділяє увагу правовим аспектам використання блокчейну для захисту традиційних знань та традиційних виражень культури корінних народів. Технологія може забезпечити захист таких нематеріальних активів від неправомірного привласнення та комерційної експлуатації, а також гарантувати справедливий розподіл вигод від їх використання [120].

Загалом, діяльність WIPO демонструє потенціал блокчейну для трансформації систем захисту прав інтелектуальної власності. Рекомендації та дослідження організації створюють основу для розвитку законодавства та міжнародної гармонізації підходів до використання блокчейну у сфері інтелектуальної власності.

Міжнародна координація регулювання блокчейн-технологій реалізується через систему взаємодії між різними організаціями, регуляторами та галузевими асоціаціями. Ефективність такої координації має критичне значення для формування узгодженого підходу до регулювання транскордонних блокчейн-відносин [117, 122].

Центральну роль у координації регуляторних підходів відіграють глобальні фінансові інституції. Світовий банк та МВФ розробляють рекомендації щодо інтеграції блокчейн-технологій у фінансову систему, особливо в контексті розвитку CBDC та модернізації платіжних систем [52, 113]. Їхні дослідження та технічна допомога сприяють формуванню узгоджених підходів до регулювання.

FSB відіграє ключову роль у координації підходів до регулювання криптоактивів на глобальному рівні. У 2022 році FSB опублікувала пропозиції щодо регулювання діяльності, пов'язаної з криптоактивами, та глобальних стандартів стейблкоїнів. Ці рекомендації, розроблені у співпраці з FATF, IOSCO та Базельським комітетом з банківського нагляду, спрямовані на забезпечення фінансової стабільності, захисту споживачів та запобігання регуляторному арбітражу у сфері криптоактивів [122].

OECP забезпечує платформу для обміну досвідом та координації політик між розвиненими країнами. Організація працює над розробкою єдиних підходів до

оподаткування операцій з віртуальними активами, впровадження механізмів обміну інформацією та протидії ухиленню від оподаткування [19, 94].

Важливу роль у формуванні узгодженого підходу до регулювання блокчейн-технологій відіграє Глобальна мережа інновацій фінансових технологій (GFIN), створена за ініціативою британського Управління з фінансової поведінки (FCA). Ця мережа об'єднує регуляторів з понад 60 країн для координації підходів до регулювання фінтех-інновацій, включаючи блокчейн [19]. GFIN забезпечує платформу для обміну досвідом, проведення крос-юрисдикційних тестів інноваційних рішень та розробки спільних регуляторних підходів. Одним із ключових напрямів діяльності мережі є гармонізація підходів до регуляторних "пісочниць" та експериментальних режимів для блокчейн-проєктів.

Значну роль у координації регулювання відіграють регіональні об'єднання. ЄС через MiCA [68] та інших регуляторних ініціатив формує модель наднаціонального регулювання, яка може стати орієнтиром для інших регіонів. ASEAN та MERCOSUR також розвивають механізми координації у сфері блокчейн-технологій [122].

ЮНСІТРАЛ працює над розробкою модельних законів, що могли б стати основою для гармонізації законодавства різних країн у сфері електронної комерції та цифрових транзакцій [138]. Такі модельні закони особливо важливі для забезпечення правової визначеності у транскордонних блокчейн-відносинах.

Важливим елементом координації є діяльність FATF. Організація не лише розробляє стандарти, але й забезпечує моніторинг їх впровадження, що створює механізм координації національних політик у сфері моніторингу [99].

Окремим напрямом міжнародної координації є взаємодія між національними регуляторами через двосторонні та багатосторонні меморандуми про взаєморозуміння. Такі угоди встановлюють механізми співпраці та обміну інформацією між наглядовими органами різних країн, що особливо важливо для ефективного нагляду за транскордонною діяльністю блокчейн-компаній [113].

Водночас чинні механізми координації стикаються з певними викликами, зокрема через різні підходи до регулювання в різних юрисдикціях, складність

забезпечення ефективного нагляду за децентралізованими системами та необхідність збалансування інтересів різних груп стейкхолдерів [96, 130].

Особливим викликом є координація підходів до регулювання DeFi та DAO, які за своєю природою функціонують поза традиційними юрисдикційними межами. Забезпечення ефективного регулювання таких систем вимагає розробки нових форм міжнародної взаємодії та інноваційних механізмів нагляду [63].

Перспективним напрямом розвитку міжнародної координації є використання самої технології блокчейн для створення систем регуляторного моніторингу та обміну інформацією. Такі системи могли б забезпечити автоматизований обмін даними між національними регуляторами, оперативне виявлення підозрілих транзакцій та ефективний нагляд за дотриманням міжнародних стандартів [144].

Стандарти та рекомендації міжнародних організацій створюють основу для розвитку конкретних механізмів захисту прав учасників блокчейн-відносин, імплементація яких відбувається через національні правові системи. Аналіз цих механізмів дозволяє оцінити ефективність різних регуляторних підходів та визначити найкращі практики для подальшої гармонізації.

3.2. Захист прав учасників та регулювання нових форм блокчейн-відносин

Міжнародна практика захисту прав учасників блокчейн-відносин формує багаторівневу систему, що поєднує традиційні правові механізми з інноваційними технологічними рішеннями [82, 97]. Основу цієї системи складають: механізми забезпечення прозорості та розкриття інформації при проведенні ICO та випуску токенів [63, 65]; механізми ідентифікації та верифікації учасників для протидії зловживанням [112, 113]; спеціалізовані механізми вирішення спорів, включаючи арбітражні платформи [25, 64]; режими захисту персональних даних через псевдонімізацію та шифрування [89, 96]; та захист прав інтелектуальної власності через токенізацію прав та автоматизоване ліцензування [73, 111].

При цьому зберігаються виклики у сфері захисту прав учасників, зокрема пов'язані з транскордонним характером блокчейну, складністю забезпечення виконання судових рішень та необхідністю балансування різних інтересів.

Захист прав інвесторів у блокчейн-проєктах суттєво різняться між юрисдикціями [48, 63]. Судова практика США створює важливі прецеденти у цій сфері, зокрема справа SEC v. Ripple Labs, що встановила диференційований підхід до токенів залежно від контексту їх продажу, та Kleiman v. Wright, яка визначила принципи визнання прав на криптоактиви в контексті спадкування [41, 43].

ЄС через MiCA запроваджує комплексну систему захисту прав інвесторів, що включає вимоги до емітентів криптоактивів щодо розкриття інформації, забезпечення фінансової стабільності та захисту від маніпуляцій на ринку. Особлива увага приділяється захисту непрофесійних інвесторів через встановлення лімітів інвестування та вимог до інформування про ризики [68].

Швейцарський регулятор розробив диференційований підхід до регулювання різних видів токенів, що дозволяє забезпечити належний рівень захисту інвесторів залежно від природи активу. При цьому значна увага приділяється прозорості проєктів та впровадженню механізмів управління ризиками [19, 66].

Сінгапур впровадив систему регулювання, що поєднує гнучкість із суворими вимогами щодо захисту інвесторів. MAS вимагає від операторів платформ впровадження механізмів перевірки проєктів та захисту коштів інвесторів [67].

Важливим елементом захисту прав інвесторів є впровадження механізмів due diligence та технічного аудиту смарт-контрактів. Міжнародна практика демонструє формування стандартів проведення таких перевірок, що мають забезпечити виявлення потенційних ризиків до здійснення інвестицій [26, 79].

Для компенсації збитків інвесторів використовуються адаптовані механізми банкрутства та реабілітації: у Японії після злому біржі Mt. Gox процедура реабілітації дозволила затвердити план виплат компенсацій 2,7 млрд доларів [113], а у США процедура банкрутства FTX демонструє можливість адаптації інструментів захисту прав кредиторів до специфіки криптоіндустрії [43].

Важливим напрямом є розвиток механізмів колективного захисту прав інвесторів. У США та ЄС формується практика групових позовів (class action) від постраждалих інвесторів криптопроєктів. Такі механізми дозволяють об'єднувати

зусилля та ресурси для ефективного судового захисту, особливо у випадках з відносно невеликими індивідуальними збитками [126, 130].

Особливої уваги заслуговує взаємодія між регулюванням криптоактивів та податковим законодавством. Різні підходи до кваліфікації криптоактивів безпосередньо впливають на їх податковий режим. У США Служба внутрішніх доходів трактує криптовалюти як майно для цілей оподаткування, що передбачає оподаткування приросту капіталу при продажу або обміні [145]. Натомість у Німеччині біткоїн та інші криптовалюти вважаються "приватними грошима", а дохід від їх продажу, що перебували у власності понад рік, звільняється від оподаткування [146]. Таке різноманіття податкових режимів створює можливості для податкового арбітражу та ускладнює захист прав інвесторів у транскордонних операціях.

Комплексний аналіз регуляторних моделей різних юрисдикцій демонструє, що ефективність захисту прав інвесторів залежить не лише від спеціального законодавства про криптоактиви, але й від його узгодженості з іншими сферами правового регулювання, зокрема податковим, корпоративним та антимонопольним законодавством [147]. Наприклад, у Швейцарії високий рівень захисту інвесторів забезпечується не лише через спеціальні норми DLT Act, але й завдяки сприятливому податковому режиму та розвиненому корпоративному законодавству, що дозволяє створювати ефективні структури для реалізації блокчейн-проєктів [19].

Водночас зберігаються виклики у сфері захисту прав інвесторів, зокрема пов'язані з характером інвестицій, складністю оцінки ризиків та необхідністю забезпечення балансу між захистом та стимулюванням інновацій [96, 122].

Захист персональних даних у блокчейн-середовищі створює виклики через конфлікт між незмінністю блокчейн-записів та правом на видалення персональних даних. Цей конфлікт гостро проявляється в контексті європейського регулювання GDPR, що закріплює "право на забуття" як право суб'єкта даних [26, 96].

Особливої складності набуває імплементація вимог GDPR у блокчейн-проєктах. Основні виклики пов'язані з визначенням ролей контролера та процесора даних у децентралізованому середовищі, забезпеченням можливості модифікації або видалення даних, а також транскордонною передачею інформації [14, 37].

Французький регулятор CNIL у 2018 році опублікував одні з перших у Європі керівних принципів щодо застосування GDPR до блокчейн-проєктів. CNIL рекомендує технічні рішення для забезпечення права на видалення даних, зокрема шифрування зі зберіганням ключів поза блокчейном, хешування та зберігання даних поза блокчейном із розміщенням у блокчейні лише посилань або хешів [38].

Британський регулятор (Information Commissioner's Office) також розробив рекомендації щодо застосування GDPR у блокчейн-проєктах. Особлива увага приділяється принципу мінімізації даних – рекомендується зберігати в блокчейні лише абсолютно необхідні персональні дані, використовувати техніки фрагментації даних (data sharding) та зашифровані посилання замість самих даних [148].

Також наголошується на важливості "privacy by design" підходу – врахування вимог захисту персональних даних на етапі проєктування блокчейн-систем. Це включає розробку архітектури, яка б забезпечувала сумісність з принципами GDPR, зокрема через використання Zero-Knowledge Proofs для верифікації даних без їх розкриття та приватних каналів для обміну чутливою інформацією [148].

Практика демонструє формування кількох підходів до розв'язання проблеми сумісності блокчейну з вимогами захисту персональних даних. Перший підхід базується на використанні off-chain сховищ, коли дані зберігаються поза блокчейном, а в реєстрі фіксуються лише хеші або посилання. Це дозволяє забезпечити можливість видалення даних без порушення цілісності блокчейну [93, 95].

Другий підхід передбачає використання механізмів псевдонімізації та шифрування. При цьому в блокчейні зберігаються лише зашифровані дані, а ключі доступу контролюються суб'єктом даних. Знищення ключів фактично робить дані недоступними, що може розглядатися як форма реалізації права на забуття [89, 91].

Третій підхід пов'язаний з розвитком технологій, що забезпечують конфіденційність, таких як Zero-Knowledge Proofs, Ring Signatures та Confidential Transactions. Ці технології дозволяють верифікувати транзакції та Smart-контракти без розкриття даних, що суттєво зменшує ризики порушення приватності [93, 96].

Особлива увага приділяється питанням передачі даних. Розвиток глобальних блокчейн-мереж вимагає забезпечення відповідності різним національним режимам

захисту персональних даних. Це створює необхідність розробки гнучких механізмів управління даними та забезпечення їх локалізації [14, 89].

У сфері фінансових послуг додаткові вимоги щодо захисту персональних даних встановлюються регуляторами. Зокрема, вимоги FATF щодо ідентифікації клієнтів мають бути збалансовані з правом на захист персональних даних [112, 113].

Для забезпечення такого балансу розробляються спеціальні протоколи, такі як Travel Rule Information Sharing Alliance (TRISA) та InterVASP Messaging Standard (IVMS101), які дозволяють провайдерам обмінюватися ідентифікаційною інформацією відповідно до вимог FATF, забезпечуючи при цьому захист даних згідно з GDPR. Ці протоколи використовують шифрування, управління доступом та мінімізацію даних для забезпечення конфіденційності при передачі інформації [99].

Разом з тим, зберігаються суттєві виклики щодо забезпечення ефективного захисту персональних даних у блокчейн-середовищі. Потрібен подальший розвиток як технічних рішень, так і правових механізмів, що забезпечували б баланс між прозорістю блокчейну та правом на приватність [96, 149].

Міжнародна практика вирішення блокчейн-спорів розвивається у двох напрямах: традиційні судові механізми та спеціалізовані форми арбітражу [83, 84]. Серед знакових судових прецедентів варто відзначити SEC v. Ripple Labs, що встановила диференційований підхід до токенів залежно від контексту їх продажу, та CFTC v. Ooki DAO, яка визначила відповідальність членів DAO за колективні рішення [41, 46]. У європейській судовій практиці акцентується увага на захисті прав споживачів та відповідності блокчейн-проєктів вимогам GDPR [26, 38].

Паралельно розвиваються арбітражні інституції, адаптовані до блокчейн-спорів: Blockchain Arbitration Forum з системою голосування токенами, платформа Jur з трирівневою системою арбітражу, а також традиційні арбітражні центри (SIAC, LCIA), які впроваджують спеціалізовані протоколи [25, 64]. Ключовою перевагою блокчейн-арбітражу є можливість автоматичного виконання рішень через смарт-контракти, що реалізується шляхом розміщення активів в escrow-смарт-контрактах або використання оракулів для передачі арбітражних рішень у блокчейн [82].

Значні виклики створює транскордонний характер блокчейн-відносин. Суди та арбітражі стикаються з необхідністю визначення юрисдикції та застосовного права у випадках, коли учасники та активи розподілені між різними юрисдикціями [96, 105].

Для розв'язання цих проблем формується практика включення у смарт-контракти та угоди про використання блокчейн-платформ чітких положень про юрисдикцію, застосовне право та механізми вирішення спорів. Ці положення можуть вказувати конкретний арбітражний суд, національну юрисдикцію або децентралізовану систему арбітражу, а також визначати процедурні аспекти вирішення спорів [96].

Важливою тенденцією є розвиток механізмів онлайн-вирішення спорів (ODR), адаптованих до специфіки блокчейн-технологій. Такі механізми забезпечують швидке та ефективне врегулювання конфліктів, хоча й створюють певні виклики щодо забезпечення виконання рішень [95, 113].

Платформи ODR, такі як Kleros, CodeLegit та Mattereum, використовують блокчейн для забезпечення прозорості процесу, незмінності доказів та автоматичного виконання рішень. Вони дозволяють проводити слухання у віртуальному середовищі, обмінюватися документами та доказами через захищені канали та залучати арбітрів з різних юрисдикцій залежно від специфіки спору [95].

Перші прецеденти визнання та приведення до виконання рішень щодо криптоактивів демонструють готовність національних судів підтримувати альтернативні механізми вирішення блокчейн-спорів. У 2019 році Верховний суд Великої Британії видав наказ про заморожування криптоактивів у справі AA v. Persons Unknown, визнавши криптовалюту майном, яке може бути об'єктом захисту. Це створило прецедент для виконання рішень, що стосуються криптоактивів [83].

Загалом, розвиток практики та спеціалізованих арбітражних механізмів створює основу для ефективного захисту прав учасників блокчейн-відносин. Поєднання традиційних правових інструментів з інноваційними технологічними рішеннями дозволяє адаптувати систему вирішення спорів до специфіки блокчейн-технологій та забезпечити адекватний рівень правового захисту у децентралізованому середовищі.

Порівняльний аналіз судових механізмів та спеціалізованих форм арбітражу для вирішення блокчейн-спорів виявляє їх відносні переваги та недоліки. Традиційні суди

забезпечують більшу правову визначеність та можливості примусового виконання рішень, але стикаються з проблемами щодо розуміння технічних аспектів та застосування наявних норм до нових ситуацій. Спеціалізовані арбітражні механізми пропонують більшу гнучкість, технічну компетентність та швидкість розгляду, але можуть зіткнутися з проблемами виконання рішень у традиційній правовій системі.

Оптимальним рішенням виглядає формування гібридних механізмів, які поєднують переваги обох підходів. Інтеграція смарт-контрактного арбітражу з традиційними механізмами, наприклад, через визнання арбітражних рішень блокчейн-платформ судами, дозволяє забезпечити ефективність. Такий підхід відображає ширшу тенденцію до конвергенції традиційних та інноваційних механізмів правового захисту у контексті цифрової трансформації.

Природа смарт-контрактів створює особливі виклики для міжнародного приватного права, що вимагає нових підходів до регулювання в різних юрисдикціях.

Аналіз міжнародного досвіду демонструє формування трьох основних підходів до правового регулювання транскордонного виконання смарт-контрактів [96, 105]. Американська модель, представлена законодавством штатів Вайомінг та Аризона, визнає смарт-контракти різновидом електронних угод, що підлягають захисту відповідно до загальних принципів договірного права [41, 67].

Європейський підхід, відображений у регламенті MiCA [68], наголошує на забезпеченні технічної надійності та прозорості автоматизованого виконання. Азійські юрисдикції, зокрема Сінгапур, зосереджуються на створенні спеціальних правових режимів для окремих видів смарт-контрактів у фінансовій сфері [66, 113].

Особливої гостроти набуває проблема визначення юрисдикції при виникненні спорів щодо виконання смарт-контрактів [82, 95]. Практика міжнародного арбітражу виявляє складність встановлення територіальної прив'язки для децентралізованих транзакцій. На відміну від традиційних договорів, де місце виконання зобов'язання часто визначає компетентний суд, у випадку смарт-контрактів виконання відбувається одночасно на всіх вузлах мережі [25, 64]. Це створює ризик конфлікту юрисдикцій та ускладнює забезпечення судового захисту.

Питання визначення юрисдикції у транскордонних спорах щодо смарт-контрактів яскраво ілюструють справи SEC v. Binance та CFTC v. Ooki DAO. У справі SEC v. Binance регулятор наполягав на юрисдикції США, оскільки платформа надавала послуги американським користувачам, попри формальну заборону та відсутність реєстрації в США. Суд підтримав позицію SEC, встановивши, що фактичне надання послуг на території США створює юрисдикційну прив'язку, попри формальні обмеження та декларації платформи [150].

У справі CFTC v. Ooki DAO регулятор притягнув до відповідальності DAO та її членів за надання послуг користувачам без відповідної реєстрації. Суд визнав, що DAO підпадає під юрисдикцію США, оскільки послуги були доступні на території США, а механізми геоблокування були неефективними. Це рішення створило важливий прецедент щодо можливості застосування національної юрисдикції до децентралізованих структур, що функціонують на глобальному рівні [151].

Для розв'язання проблеми юрисдикції у смарт-контрактах використовуються різні підходи. Один з них – включення в код або в пов'язану документацію чітких положень про юрисдикцію та право. Інший підхід передбачає використання арбітражних механізмів, які функціонують паралельно зі смарт-контрактами та забезпечують вирішення спорів поза національними юрисдикціями [82, 95].

Практика демонструє тенденцію до розвитку спеціалізованих механізмів вирішення спорів, адаптованих до специфіки смарт-контрактів [83, 84]. Показовим є досвід Швейцарії, де створено систему "криптодолини" з власними арбітражними інституціями, орієнтованими на блокчейн-спори [16, 66]. Сінгапурський міжнародний арбітражний центр розробив спеціальні протоколи для розгляду справ, пов'язаних з автоматизованим виконанням транскордонних зобов'язань [105, 113].

Важливим аспектом транскордонного виконання смарт-контрактів є питання визнання та приведення до виконання арбітражних рішень у різних юрисдикціях [39, 122]. Хоча Нью-Йоркська конвенція 1958 року створює загальну основу для визнання арбітражних рішень, її застосування до блокчейн-спорів потребує адаптації з урахуванням технологічної специфіки [25, 37]. Зокрема, виникають питання щодо можливості примусового виконання, які вимагають модифікації смарт-контракту.

Аналіз міжнародної практики виявляє формування нових підходів до забезпечення виконання смарт-контрактів [83, 145]. Суди починають визнавати технічну незворотність транзакцій та розробляють альтернативні механізми захисту прав, зокрема через компенсаційні виплати або використання нових смарт-контрактів для виправлення наслідків порушень [67, 152]. Це відображає загальну тенденцію до адаптації традиційних правових інструментів до реалій цифрової економіки.

Перспективним напрямом розвитку є впровадження гібридних механізмів виконання, що поєднують автоматизацію смарт-контрактів з елементами судового контролю [82, 117]. Такий підхід, започаткований у практиці Дубайського міжнародного фінансового центру [153, 154], передбачає можливість інтеграції арбітражних застережень безпосередньо в код смарт-контракту. Це дозволяє забезпечити баланс між технологічною ефективністю та правовою визначеністю.

Подальший розвиток виконання смарт-контрактів потребує посилення міжнародної координації та гармонізації правових підходів [96, 122]. Важливим кроком може стати розробка стандартів реалізації арбітражних механізмів у смарт-контрактах та створення спеціалізованих міжнародних платформ для вирішення блокчейн-спорів. Це сприятиме підвищенню правової визначеності та ефективності захисту прав учасників транскордонних блокчейн-відносин.

Механізми захисту прав, розроблені для традиційних блокчейн-відносин, потребують адаптації до нових форм взаємодії, що виникають у міру розвитку технології. DeFi, DAO та NFT створюють унікальні регуляторні виклики, які потребують інноваційних підходів до правового регулювання.

Нові форми блокчейн-відносин (DeFi, DAO, NFT, токенізовані активи) вимагають адаптації традиційних механізмів захисту прав та розробки спеціалізованих регуляторних підходів, що забезпечуватимуть збереження фундаментальних принципів (прозорість, інформовану згоду, доступність правового захисту) в умовах децентралізації та автоматизації.

DeFi створюють унікальні регуляторні виклики через відсутність централізованих суб'єктів, відповідальних за дотримання законодавства [104]. У

США регулятори пристосовують чинні інструменти: SEC застосовує "тест Хоуї" до DeFi-токенів, а CFTC розглядає деякі DeFi-інструменти як деривативи [18].

В останні роки SEC значно посилила нагляд за DeFi. У 2023 році регулятор розпочав розслідування щодо біржі Uniswap та подібних платформ, наполягаючи, що вони повинні реєструватися як біржі цінних паперів або альтернативні торгові системи, якщо на них торгуються токени, які відповідають критеріям інвестиційного контракту. SEC також висунула звинувачення проти творців DeFi-протоколу Forsage, кваліфікувавши його як піраміду та незареєстрований випуск цінних паперів [18].

У ЄС регулювання DeFi здійснюється в рамках загальної політики щодо криптоактивів. Ключовим документом є регламент про ринки криптоактивів (MiCA), який встановлює вимоги до емітентів токенів і VASP [68]. Хоча MiCA не містить спеціальних норм щодо DeFi, його положення про токени, забезпечені активами, та токени електронних грошей можуть застосовуватися до окремих DeFi-інструментів.

Європейські регулятори застосовують функціональний підхід до DeFi, зосереджуючись на економічній сутності послуг, а не на їх технічній реалізації. Якщо DeFi-протокол виконує функції, аналогічні традиційним фінансовим посередникам (наприклад, обмін валют, кредитування, управління активами), до нього можуть застосовуватися відповідні регуляторні вимоги. Європейська Комісія та Європейський банківський орган (EBA) визнають, що повна децентралізація є рідкістю, і зазвичай існують особи або організації, які мають значний вплив на протокол і можуть вважатися відповідальними за його функціонування [68].

У звіті "DeFi Market Trends, Risks and Regulation" (2022) IOSCO відзначає ознаки централізації в багатьох DeFi-проєктах, що дозволяє визначити відповідальних суб'єктів. IOSCO рекомендує ризик-орієнтований підхід до регулювання та міжнародну співпрацю для запобігання регуляторному арбітражу [126].

Важливим аспектом регулювання DeFi є також AML/CFT. FATF у своїх рекомендаціях закликає країни застосовувати стандарти AML/CFT до VASP [99]. Це передбачає впровадження процедур ідентифікації клієнтів (KYC), моніторинг підозрілих транзакцій і звітування перед компетентними органами.

Проблемним аспектом залишається можливість реалізації KYC-процедур у децентралізованому середовищі. Окремі DeFi-протоколи експериментують з інтеграцією рішень децентралізованої ідентифікації і верифікації користувачів через сторонні сервіси [126]. Однак уніфікованих стандартів у цій сфері поки що немає, що створює ризики для залучення DeFi-платформ до незаконної діяльності.

Сінгапур демонструє передовий підхід до регулювання DeFi, розробляючи спеціальні експериментальні режими для таких проєктів у рамках регуляторної "пісочниці" MAS. Project Guardian, започаткований у 2022 році, спрямований на тестування використання DeFi в інституційних фінансових ринках. Проєкт охоплює регульовані фінансові установи, такі як DBS Bank, JPMorgan та Marketnode, і фокусується на розробці стандартів для токенізації активів та впровадження DeFi-протоколів у традиційні фінансові операції [113].

Японія також активно розвиває регуляторні підходи до DeFi. Агентство фінансових послуг Японії розробляє специфічні вимоги для DeFi-платформ у рамках загальної системи регулювання криптоактивів. Японський підхід базується на саморегулюванні через Японську асоціацію бірж віртуальних валют, яка розробляє стандарти для DeFi-проєктів, включаючи вимоги до прозорості коду, аудиту смарт-контрактів та захисту користувачів [69].

Регулювання DeFi знаходиться на етапі становлення та потребує адаптації до реалій. Для регулювання необхідні: критерії визначення відповідальних осіб у, спеціальні правила розкриття інформації, стандарти децентралізованої ідентифікації та посилення міжнародної координації. Важливо, щоб цей процес відбувався в діалозі з індустрією для розробки збалансованих підходів.

DAO є новою формою управління та координації економічної діяльності, що базується на блокчейн-технологіях і смарт-контрактах. DAO функціонують без традиційної ієрархічної структури, а рішення в них ухвалюються шляхом голосування учасників відповідно до закладених у протоколі правил [100]. Такі організації можуть виконувати різноманітні функції: від управління інвестиційними фондами до координації роботи децентралізованих платформ і сервісів.

Правовий статус DAO залишається невизначеним у більшості юрисдикцій. Проблема полягає в тому, що DAO не вписуються в традиційні організаційно-правові форми (товариства, асоціації тощо), а їхня децентралізована природа ускладнює застосування наявних норм корпоративного та договірного права [63].

У США підходи до визначення правового статусу DAO різняться залежно від штату. У 2021 році Вайомінг став першим штатом, який на законодавчому рівні визнав DAO як окрему організаційно-правову форму (DAO LLC) [67]. Закон Вайомінгу про DAO LLC визначає DAO як товариство з обмеженою відповідальністю, організоване відповідно до законодавства Вайомінгу, управління яким здійснюється повністю або частково через смарт-контракти учасниками, які голосують алгоритмічно верифікованими токенами.

Закон встановлює спрощену процедуру створення DAO LLC, дозволяючи реєструвати організацію з мінімальними формальностями. Статут DAO може бути представлений у вигляді смарт-контракту, а управління може здійснюватися через блокчейн. При цьому DAO LLC отримує правосуб'єктність та обмежену відповідальність учасників, які не несуть особистої відповідальності за DAO.

Подібні законодавчі ініціативи розглядаються і в інших штатах, таких як Делавер і Теннессі, які прагнуть створити сприятливе правове середовище для розвитку DAO.

На федеральному рівні DAO можуть кваліфікуватися як інвестиційні компанії або емітенти цінних паперів, якщо вони відповідають критеріям "тесту Хоуі". У такому разі на них поширюються вимоги щодо реєстрації та розкриття інформації, передбачені законодавством про цінні папери [41].

Показовою у цьому контексті є справа CFTC v. Ooki DAO (2022), в якій CFTC притягнула до відповідальності DAO та її учасників за надання послуг з торгівлі товарними деривативами без належної реєстрації. CFTC визначила, що Ooki DAO є асоціацією відповідно до законодавства Каліфорнії, а "виборці" DAO несуть персональну відповідальність за її діяльність. Суд підтримав позицію CFTC, створивши важливий прецедент щодо відповідальності членів DAO за порушення регуляторних вимог [151].

У ЄС немає спеціального регулювання DAO, але окремі аспекти їхньої діяльності можуть підпадати під дію наявних норм. Зокрема, якщо DAO здійснює емісію токенів, які кваліфікуються як криптоактиви, застосовними можуть бути положення MiCA [68]. У разі надання фінансових послуг DAO повинні дотримуватися відповідних вимог директив про платіжні послуги, про ринки фінансових інструментів та AML.

Європейські регулятори схиляються до функціонального підходу, фокусуючись на фактичній діяльності DAO, а не на її формальній структурі. Якщо DAO виконує функції фінансового посередника, вона повинна дотримуватися відповідних вимог, незалежно від своєї природи. При цьому відповідальність за дотримання вимог може покладатися на фактичних контролерів DAO, таких як розробники, власники токенів управління чи особи, які мають значний вплив на її діяльність [68].

Мальта, яка позиціює себе як блокчейн-острів, у 2019 році прийняла закон про інноваційні технологічні послуги, який передбачає можливість реєстрації DAO як "інноваційних технологічних послуг" [67]. Це дозволяє DAO набувати правосуб'єктності та здійснювати діяльність під наглядом мальтійського регулятора.

В Азії особливої уваги заслуговує досвід Сінгапуру, де MAS зайняло проактивну позицію щодо регулювання DAO. MAS розглядає DAO як важливий елемент розвитку децентралізованих систем і працює над створенням експериментального регуляторного середовища для їх тестування [119]. Зокрема, обговорюється можливість надання DAO статусу обмеженого партнерства (limited partnership) з відповідними вимогами до розкриття інформації та управління ризиками.

Важливим аспектом регулювання DAO є визначення їхнього податкового статусу. У більшості юрисдикцій DAO не мають спеціального податкового режиму і розглядаються відповідно до загальних правил оподаткування юридичних осіб або партнерств. У США, наприклад, DAO можуть вважатися корпораціями, партнерствами або іншими юридичними формами для цілей оподаткування, залежно від їхньої структури та характеру діяльності [67].

Оподаткування DAO ускладнюється їхньою природою, коли члени організації та її активи розподілені між різними юрисдикціями. Це створює ризики подвійного

оподаткування або уникнення податків. Для розв'язання цих проблем необхідна міжнародна координація та гармонізація підходів до оподаткування DAO.

Регулювання DAO перебуває на початковому етапі, і країни тільки формують підходи до визначення їхнього статусу. Пріоритетними напрямами є: розробка спеціальних організаційно-правових форм, визначення критеріїв правосуб'єктності DAO, механізми захисту прав учасників, забезпечення дотримання вимог AML/CFT та гармонізація підходів на міжнародному рівні. Ефективне регулювання потребує балансу між стимулюванням інновацій та забезпеченням безпеки учасників.

NFT є особливим видом криптоактивів, які представляють право власності на унікальні цифрові об'єкти (зображення, відео, аудіо тощо). На відміну від традиційних токенів, NFT не є взаємозамінними та мають власну цінність, обумовлену рідкісністю та попитом на конкретний цифровий актив [71].

Поширення NFT у таких сферах, як цифрове мистецтво, колекціонування та ігрова індустрія, актуалізувало питання їх регулювання. Основними викликами є визначення правової природи NFT, захист прав інтелектуальної власності, оподаткування, а також запобігання шахрайству та маніпулюванню на ринку [79].

У більшості юрисдикцій NFT не мають окремого правового статусу і розглядаються в рамках загального регулювання криптоактивів. У США підходи до кваліфікації NFT різняться залежно від контексту їх використання. SEC аналізує NFT на предмет відповідності критеріям цінних паперів за "тестом Хоуї". Якщо NFT надають право на отримання прибутку від діяльності емітента або передбачають розподіл доходів між власниками, вони можуть розглядатися як інвестиційні контракти та підпадати під дію законодавства про цінні папери [109].

Особливої уваги регуляторів заслуговують випадки фракціонування NFT, коли право власності на токен розділяється між кількома інвесторами. SEC висловила занепокоєння щодо таких практик, оскільки фракціоновані NFT можуть мати ознаки інвестиційних контрактів. У 2023 році регулятор розпочав розслідування щодо проєкту Yuga Labs, творця колекції Bored Ape Yacht Club, зокрема аналізуючи правову природу ApeCoin та фракціонованих NFT, пов'язаних з проєктом [109].

Якщо ж NFT є унікальними цифровими предмети без інвестиційного компонента, вони можуть кваліфікуватися як товари з відповідними наслідками. У 2022 році Управління з внутрішніх доходів США опублікувало керівні принципи щодо оподаткування операцій з NFT, кваліфікувавши їх як "колекційні цифрові активи" для цілей оподаткування приросту капіталу [145].

У ЄС NFT можуть підпадати під дію MiCA, якщо вони відповідають визначенню криптоактиву [68]. Водночас MiCA передбачає винятки для деяких токенів, зокрема тих, що представляють унікальні нефінансові активи (предмети колекціонування, цифрові предмети в іграх тощо). Стаття 2(4) MiCA виключає з-під дії регламенту "криптоактиви, які є унікальними та не взаємозамінними з іншими криптоактивами".

Однак Європейська Комісія уточнила, що виняток не поширюється на NFT, які мають характеристики та прирівнюються до взаємозамінних активів. Якщо колекція містить кілька токенів з однаковими функціями та властивостями, вона може розглядатися як серія активів, а не як сукупність унікальних NFT. У такому випадку до неї можуть застосовуватися вимоги MiCA щодо емісії та обігу [68].

Важливим аспектом регулювання NFT є також захист прав інтелектуальної власності. Оскільки NFT часто представляють цифрові об'єкти, захищені авторським правом (зображення, музику, відео), необхідно забезпечити дотримання прав авторів та запобігати несанкціонованому використанню їхніх творів [120].

У цьому контексті показовою є справа Hermès v. MetaBirkins, в якій французький люксовий бренд успішно позивався проти цифрового художника, який створив колекцію NFT із зображеннями віртуальних сумок, схожих на культову модель Birkin. Суд Південного округу Нью-Йорка визнав, що використання бренду Birkin у назві колекції NFT порушує права на торгову марку, а самі зображення не захищені Першою поправкою, оскільки мають переважно комерційний, а не художній характер. Це рішення стало важливим прецедентом щодо застосування традиційного законодавства про інтелектуальну власність до NFT [127].

Іншим резонансним випадком є справа Miramax v. Tarantino, де кінокомпанія Miramax подала позов проти режисера Квентіна Тарантіно через його плани продати NFT, пов'язані з фільмом "Кримінальне чтиво". Miramax стверджувала, що має

виключні права на дистрибуцію фільму, тоді як Тарантіно наполягав, що зберіг за собою певні права, включаючи право на публікацію сценарію. Сторони врешті досягли позасудового врегулювання, але справа привернула увагу до складних питань розподілу прав при створенні NFT на основі наявних творів [109].

Підходи до регулювання NFT демонструють різні акценти й пріоритети. Франція визначила NFT як цифрові активи та встановила вимоги до емітентів зі створенням спеціального реєстру. Японія запровадила реєстрацію NFT, що представляють права на реальні активи, як сертифікатів із відповідними вимогами. Підходи до оподаткування також варіюються: від трактування NFT як цифрових активів до застосування режиму оподаткування базового активу при токенізації цінностей [73].

Перспективним напрямом є також регулювання токенізованих активів — цифрових токенів, які представляють право власності на реальні активи (акції, облігації, сировинні товари тощо). Токенізація дозволяє підвищити ліквідність та доступність традиційних активів, а також спростити їх транскордонний обіг [93]. Водночас вона створює нові виклики для регуляторів, пов'язані з узгодженням правового режиму токенізованих активів із вимогами до обігу базових активів.

У США SEC розглядає більшість токенізованих активів як цінні папери, що підлягають реєстрації та регулюванню відповідно до федерального законодавства [41]. У ЄС токенізовані активи можуть підпадати під дію регламенту про ринки криптоактивів (MiCA) або спеціального режиму для цінних паперів на блокчейні, який планується запровадити найближчим часом [128].

Регламент DLT pilot regime, прийнятий у ЄС у 2022 році, створює експериментальний режим для розвитку інфраструктури ринку цінних паперів на базі технології розподіленого реєстру. Він дозволяє операторам ринкової інфраструктури (біржам та депозитаріям) використовувати блокчейн для обслуговування токенізованих цінних паперів, з можливістю тимчасових відступів від окремих вимог традиційного регулювання фінансових ринків [68].

Загалом, регулювання NFT та токенізованих активів перебуває на початковому етапі, і країни тільки починають формувати підходи до визначення їхнього статусу та встановлення правил обігу. Ключовими напрямами вдосконалення регулювання є:

- Розробка критеріїв класифікації NFT та токенізованих активів.
- Впровадження механізмів захисту прав інтелектуальної власності.
- Встановлення вимог до емітентів NFT і токенізованих активів щодо розкриття інформації, управління ризиками та захисту прав інвесторів.
- Гармонізація підходів до оподаткування операцій з NFT.
- Забезпечення дотримання вимог AML/CFT.

Важливо, щоб регулювання NFT і токенізованих активів здійснювалося з урахуванням їх технологічних особливостей та економічних функцій. Надмірно жорсткі обмеження можуть стримувати розвиток інноваційних моделей токенізації та використання блокчейну для представлення прав на унікальні цифрові об'єкти. Водночас відсутність базових правил створює ризики для учасників ринку та може призвести до зловживань. Пошук збалансованого підходу вимагає активного діалогу між регуляторами, експертами з блокчейну та представниками індустрії.

Розвиток блокчейн-технологій та поширення DApps створюють нові виклики для захисту конкуренції та запобігання монополізації ринку. З одного боку, блокчейн сприяє прозорості, зниженню бар'єрів для входу на ринок та усуненню посередників, що має позитивний вплив на конкурентне середовище. З іншого боку, особливості функціонування блокчейн-мереж можуть призводити до концентрації влади в руках окремих учасників та створювати ризики антиконкурентної поведінки [154].

Одним із ключових викликів є забезпечення доступу до інфраструктури блокчейну. В PoW та PoS системах виникають ризики концентрації влади, що створює потенційні загрози для конкуренції та децентралізації [28].

Показовим прикладом антимонопольного розслідування в цій сфері стала справа Європейської Комісії щодо картельної змови між майнінговими пулами Ethereum у 2022 році. Регулятор аналізував можливість координації між пулами для оптимізації винагород, що могло порушувати статтю 101 Договору про функціонування Європейського Союзу, яка забороняє картельні угоди. Це розслідування вперше порушило питання про застосування антимонопольних норм до децентралізованих форм координації економічної поведінки в блокчейн-мережах [122].

Іншим викликом є забезпечення сумісності та взаємодії між блокчейн-мережами. Відсутність протоколів взаємодії може призводити до фрагментації ринку та створювати штучні бар'єри [45]. Це актуально для сфери DeFi, де сумісність протоколів є умовою формування ефективної екосистеми фінансових послуг.

Проблемою є також потенційне зловживання панівним становищем з боку великих блокчейн-компаній та консорціумів. Зокрема, існують побоювання, що провідні технологічні корпорації можуть використовувати свої ресурси та мережеві ефекти для монополізації окремих сегментів блокчейн-індустрії [122]. Це може проявлятися у нав'язуванні власних стандартів, обмеженні доступу до ключових інфраструктурних компонентів або встановленні завищених цін на послуги.

У 2023 році Федеральна торгова комісія США (FTC) розпочала розслідування щодо криптобіржі Coinbase за можливе зловживання становищем. Регулятор аналізував практики біржі щодо маніпулювання комісіями та обмеження доступу конкурентів до інфраструктури. Це розслідування демонструє застосування інструментів антимонопольного регулювання до криптовалютного ринку [129].

Японський антимонопольний орган у 2022 році провів розслідування щодо практик великих криптобірж з обмеження лістингу токенів малих проєктів. Розслідування завершилося прийняттям учасниками ринку добровільних зобов'язань щодо забезпечення прозорих та недискримінаційних умов доступу до торгових платформ. Це демонструє можливість застосування інструментів антимонопольного регулювання для розв'язання проблем конкуренції на криптовалютних ринках [69].

Аналіз практики антимонопольних органів демонструє формування специфічних підходів до оцінки концентрації та узгоджених дій на ринках, пов'язаних з блокчейн-технологіями. Зокрема, при визначенні ринкової влади враховуються такі особливі фактори, як контроль над протоколом, частка в майнінгу або стейкінгу, володіння ключовою інтелектуальною власністю та мережеві ефекти [129]. Блокчейн-консорціуми, які об'єднують конкурентів для спільної розробки технологічних стандартів, оцінюються з погляду їх впливу на інновації та бар'єри входу на ринок.

Дослідження взаємодії блокчейн-регулювання з антимонопольним правом виявляє важливий баланс: надто жорстке регулювання створює передумови для

монополізації (як у випадку BitLicense в Нью-Йорку), а надто ліберальний підхід може сприяти формуванню природних монополій через мережеві ефекти. Оптимальна модель має забезпечувати баланс між безпекою та конкуренцією [44].

Швейцарська Комісія з питань конкуренції у 2021 році прийняла рішення щодо допустимості блокчейн-консорціумів у банківському секторі, встановивши критерії оцінки таких об'єднань з погляду антимонопольного законодавства. Комісія визначила, що блокчейн-консорціуми можуть вважатися допустимими, якщо вони забезпечують доступ для нових учасників, використовують стандартизовані протоколи взаємодії та не обмежують конкуренцію на суміжних ринках [113].

Конкуренція юрисдикцій за залучення блокчейн-проєктів також становить виклик для гармонізації регулювання. Деякі країни свідомо пільгові режими для криптобізнесу, що може підривати ефективність стандартів та створювати ризики регуляторного арбітражу [67]. Така "гонитва" у стандартах регулювання може призводити до концентрації ризиків у юрисдикціях з найбільш ліберальними підходами та створювати загрози для глобальної фінансової стабільності.

Для вирішення цих викликів антимонопольні органи різних країн починають розробляти підходи до регулювання конкуренції в блокчейн-середовищі. У США Федеральна торгова комісія (FTC) приділяє особливу увагу дослідженню впливу блокчейн-технологій на конкуренцію та захист прав споживачів [129]. FTC розглядає можливість застосування традиційних інструментів антимонопольного регулювання, таких як контроль за злиттями та поглинаннями, до блокчейн-компаній, а також розробляє нові підходи, адаптовані до специфіки децентралізованих мереж.

У ЄС питання конкуренції в блокчейн-середовищі розглядаються в контексті цифрових ринків. Європейська комісія визнає потенціал блокчейну для підвищення прозорості та ефективності ринків, але водночас наголошує на необхідності запобігання антиконкурентним практикам [37]. Зокрема, Комісія досліджує ризики змови між учасниками, потенційне зловживання панівним становищем з боку технологічних гігантів, а також питання сумісності та доступу до даних.

Важливим напрямом розвитку конкурентної політики в блокчейн-середовищі є також міжнародна співпраця та гармонізація підходів. Глобальний характер

блокчейн-мереж вимагає узгоджених дій антимонопольних органів різних країн для запобігання транскордонним антиконкурентним практикам [122]. Це передбачає обмін інформацією, проведення спільних розслідувань та вироблення спільних стандартів оцінки впливу блокчейн-технологій на конкуренцію.

Перспективним інструментом захисту конкуренції в блокчейн-середовищі є також саморегулювання та розвиток галузевих стандартів. Блокчейн-спільнота може відігравати роль у виробленні правил чесної конкуренції, забезпеченні прозорості та недискримінаційного доступу до інфраструктури [50].

Блокчейн-технологія стає інструментом запобігання недобросовісній конкуренції та підвищення прозорості. Прикладами є платформа IBM Food Trust для простежуваності продуктів, система De Beers Tracr для відстеження походження алмазів та проєкт ЄС Blockchers для захисту географічних зазначень [107].

Захист конкуренції в блокчейн-середовищі вимагає підходу, що поєднує традиційні інструменти антимонопольного регулювання з новими механізмами, адаптованими до специфіки децентралізованих мереж. Ключовими напрямами є: забезпечення рівного доступу, сприяння стандартизації та сумісності, моніторинг зловживань, розвиток співпраці та стимулювання саморегулювання галузі.

Аналіз регулювання нових форм блокчейн-відносин свідчить, що цей процес знаходиться на початковому етапі розвитку з різноманітними національними підходами. Викликами залишаються: визначення відповідальних суб'єктів, розвиток функціонального підходу, орієнтованого на економічну сутність діяльності, забезпечення співпраці між регуляторами та індустрією, а також міжнародна координація для запобігання фрагментації правового поля. Розрізненість національного регулювання актуалізує питання міжнародної гармонізації для забезпечення ефективного транскордонного функціонування блокчейн-екосистеми.

3.3. Перспективи міжнародної гармонізації регулювання блокчейн-технологій

Характер блокчейн-технологій вимагає міжнародної координації регуляторних підходів, оскільки фрагментарність національного регулювання створює ризики

арбітражу, ускладнює протидію незаконним практикам і стримує розвиток інновацій, що зумовлює необхідність формування узгоджених міжнародних стандартів.

Аналіз поточного стану міжнародної гармонізації демонструє значні відмінності в підходах різних юрисдикцій до регулювання блокчейн-технологій. Ці відмінності проявляються у класифікації криптоактивів, вимогах до ліцензування та нагляду, підходах до захисту споживачів та інвесторів, а також у механізмах AML/CFT [96].

З теоретичного погляду, міжнародна гармонізація регулювання блокчейн-технологій відображає концепцію "багаторівневого управління", розроблену Г. Марксом та Л. Хугом [136]. Відповідно до цієї концепції, регуляторна компетенція розподіляється між різними рівнями — глобальним (FATF, IOSCO), регіональним (ЄС, ASEAN) та національним — з різним ступенем обов'язковості та деталізації норм. У сфері блокчейн-технологій така модель управління проявляється через взаємодію між "м'яким правом" міжнародних організацій та "жорстким правом" національних юрисдикцій, причому ефективність гармонізації залежить від ступеня конвергенції цих регуляторних рівнів.

Водночас спостерігається формування міжнародних стандартів та рекомендацій, що створюють основу для гармонізації національних підходів. Ключову роль у цьому процесі відіграють міжнародні організації, такі як FATF, IOSCO, FSB, ISO та інші, які розробляють глобальні стандарти у своїх сферах компетенції [50, 99, 126].

Значного прогресу досягнуто у сфері AML/CFT. Рекомендації FATF щодо віртуальних активів та VASP імплементовані в національне законодавство більшості розвинених країн [99]. Водночас зберігаються відмінності в підходах до технічної реалізації цих вимог, зокрема щодо "правила подорожі" та ідентифікації клієнтів.

У сфері захисту прав інвесторів та споживачів спостерігається менша узгодженість. Різні юрисдикції по-різному класифікують криптоактиви та встановлюють вимоги до їх емісії та обігу. Наприклад, США застосовують законодавство про цінні папери до більшості інвестиційних токенів, тоді як ЄС розробив режим для криптоактивів у рамках регламенту MiCA [41, 68].

Особливо складною є гармонізація підходів до нових форм блокчейн-відносин, таких як DeFi, DAO та NFT. Ці інноваційні форми часто не вписуються в традиційні

регуляторні рамки та вимагають розробки нових, адаптованих до їх специфіки підходів. При цьому різні юрисдикції демонструють різний рівень готовності до експериментів та інновацій у регуляторній сфері [96].

Ініціативи G20 та FSB відіграють роль у координації глобальних підходів до регулювання криптоактивів. У 2022 році FSB опублікувала пропозиції щодо регулювання діяльності, пов'язаної з криптоактивами, та глобальних стандартів. Ці рекомендації, розроблені у співпраці з FATF, IOSCO та Базельським комітетом з банківського нагляду, спрямовані на забезпечення фінансової стабільності, захисту споживачів та запобігання регуляторному арбітражу у сфері криптоактивів [122].

МВФ та Світовий банк також працюють над розробкою рекомендацій для країн, що розвивають законодавство про блокчейн. Вони надають технічну допомогу, проводять дослідження та розробляють керівні принципи для регуляторів. Особлива увага приділяється питанням фінансової стабільності, захисту прав споживачів та забезпечення інклюзивного доступу до фінансових послуг [122].

Імплементацію міжнародних стандартів ускладнюють: різноманітність правових систем, термінологічні розбіжності між юрисдикціями [99], технологічні бар'єри при впровадженні "правила подорожі" [101] та складність забезпечення транскордонного нагляду [113]. Ключову роль у подоланні цих викликів відіграють регіональні ініціативи: ЄС з комплексною системою регламентів (MiCA) та Європейською інфраструктурою блокчейн-сервісів [68, 128], ASEAN з регіональними принципами використання блокчейну в платіжних системах [122], а також регіональні форуми, як-от APEC, що забезпечують обмін досвідом між регуляторами.

Для порівняльного аналізу ефективності регуляторних моделей доцільно застосувати багатокритеріальний підхід, що враховує: інноваційність (здатність сприяти розвитку блокчейн-рішень), захист прав учасників, забезпечення фінансової стабільності, адаптивність до технологічних змін та міжнародну сумісність [87, 135].

Аналіз демонструє, що найбільш ефективними є відкрито-ліберальні юрисдикції (Швейцарія, Сінгапур, Ліхтенштейн), які забезпечують баланс між інноваціями та публічними інтересами [135]. Емпіричні дані підтверджують: у швейцарському кантоні Цуг з 2018 по 2022 рік кількість блокчейн-компаній зросла на 177%, а

капіталізація провідних проєктів досягла 185 млрд швейцарських франків [137]. При цьому рівень виявлених порушень AML-законодавства залишається низьким [138].

Ключовими факторами ефективності є: правова визначеність, пропорційність вимог, технологічна нейтральність та проактивність. Важливу роль відіграють також експериментальні механізми та якість діалогу між регуляторами та індустрією [87, 96]. Помірковано-регульовані юрисдикції (США, ЄС) забезпечують вищий рівень захисту споживачів, але можуть створювати бар'єри для невеликих інноваційних проєктів, тоді як жорстко-рестриктивні підходи (Китай) ефективно контролюють ризики, але не сприяють децентралізованим інноваціям [135].

Ефективне регулювання блокчейну вимагає комплексного підходу:

- Чітку правову визначеність щодо статусу криптоактивів;
- Пропорційні вимоги до учасників ринку;
- Ефективні механізми нагляду та контролю;
- Міжнародну координацію та обмін інформацією.

На основі порівняльного аналізу ефективності різних регуляторних моделей можна визначити найкращі практики та рекомендації для формування оптимальної системи регулювання блокчейн-технологій. Ці рекомендації можуть стати основою для міжнародної гармонізації підходів та розвитку глобальних стандартів.

Оптимальною моделлю для глобальної регуляторної екосистеми блокчейн-технологій є багаторівневе регулювання, що поєднує глобальні стандарти (FATF, ISO, FSB), регіональні правила (ЄС, ASEAN) та національні підходи з урахуванням специфіки правових систем. Елементами цієї екосистеми мають стати механізми координації між регуляторами, технологічні рішення та саморегулювання індустрії через галузеві асоціації та технічні консорціуми [139, 140].

Аналіз тенденцій дозволяє виділити три ймовірні сценарії міжнародної гармонізації: поступова конвергенція (2025-2027) через імплементацію глобальних стандартів; регіональна гармонізація (2025-2030) з формуванням регуляторних блоків та механізмів взаємного визнання; фрагментація з "мостами" (2025-2028) зі збереженням національних особливостей та розвитком механізмів транскордонної

взаємодії [87, 122]. Найбільш імовірним на поточному етапі виглядає сценарій регіональної гармонізації, що відповідає загальним тенденціям розвитку глобального фінансового регулювання. Успішність цього процесу залежить від здатності міжнародної спільноти знайти баланс між стимулюванням інновацій, захистом прав споживачів та забезпеченням фінансової стабільності.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. Проведений порівняльно-правовий аналіз міжнародного досвіду регулювання блокчейн-технологій демонструє динамічний процес формування регуляторних підходів, що еволюціонують від фрагментарного регулювання до системних моделей, адаптованих до технологічної специфіки децентралізованих систем.

2. Аналіз підходів різних юрисдикцій виявив формування трьох основних типів регулювання: відкрито-ліберального, помірковано-регульованого та жорстко-рестриктивного. Встановлено, що на вибір регуляторної моделі впливають не лише технологічні особливості блокчейну, але й соціально-економічні та політичні фактори, включаючи традиції правової системи, пріоритети державної політики та підходи до інновацій.

3. Аналіз діяльності міжнародних організацій виявив їх ключову роль у формуванні глобальних стандартів та координації регуляторних підходів. Встановлено, що найбільш значного прогресу досягнуто у сфері протидії відмиванню коштів завдяки діяльності FATF, технічна стандартизація здійснюється ISO/TC 307, а WIPO, IOSCO, FSB та інші організації формують стандарти у своїх сферах компетенції.

4. Дослідження імплементації рекомендацій FATF виявило нерівномірність впровадження "правила подорожі", зумовлену як технічними викликами, так і відмінностями правових систем. Встановлено, що ефективність імплементації залежить від узгодженості нормативних вимог з технічними можливостями та забезпечення балансу між прозорістю транзакцій і захистом персональних даних.

5. Дослідження механізмів захисту прав учасників блокчейн-відносин виявило формування комплексної системи, що поєднує традиційні правові інструменти з

інноваційними технологічними рішеннями. Проаналізовано механізми захисту прав інвесторів, розвиток спеціалізованих арбітражних інституцій та форм онлайн-вирішення спорів, адаптованих до специфіки блокчейн-технологій.

6. Аналіз стандартів захисту персональних даних виявив фундаментальний конфлікт між незмінністю блокчейн-записів та правом на видалення персональних даних за GDPR. Досліджено технічні рішення для забезпечення сумісності блокчейну з вимогами захисту персональних даних, включаючи off-chain сховища, механізми псевдонімізації та шифрування.

7. Дослідження регулювання нових форм блокчейн-відносин (DeFi, DAO, NFT) демонструє формування спеціалізованих регуляторних підходів, адаптованих до їх технологічної та економічної специфіки. Виявлено тенденцію до функціонального регулювання, що фокусується на економічній сутності послуг, а не на технічних особливостях їх реалізації.

8. Аналіз підходів до регулювання DeFi виявив виклики, пов'язані з відсутністю централізованих суб'єктів. Дослідження статусу DAO в різних юрисдикціях виявило різноманітність підходів: від спеціалізованих організаційно-правових форм до кваліфікації як традиційних партнерств. Аналіз регулювання NFT та токенізованих активів виявив різноманітність національних підходів до їх правової кваліфікації.

9. Дослідження перспектив міжнародної гармонізації регулювання блокчейн-технологій виявило тенденцію до формування глобальної регуляторної екосистеми, що поєднує глобальні стандарти, регіональні правила та національні підходи. Найбільш імовірним є сценарій регіональної гармонізації з формуванням регуляторних блоків, що відповідає загальним тенденціям розвитку міжнародного фінансового регулювання.

Р О З Д І Л 4. Напрямки вдосконалення правового регулювання блокчейн-технологій в Україні

4.1. Концептуальні основи та модернізація матеріально-правового регулювання

Концепція регулювання блокчейн-технологій ґрунтується на поєднанні саморегулювання, співрегулювання та державного нагляду з акцентом на адаптивність. Центральним елементом є перехід від статичного до динамічного, принцип-орієнтованого підходу, що забезпечує баланс між регуляторною визначеністю та стимулюванням інновацій. Ключовими концептуальними принципами є технологічна нейтральність та захист прав учасників при врахуванні технічних особливостей блокчейну, описаних у Розділі 1.

Технологічна нейтральність є ключовим принципом сучасного правового регулювання інформаційних технологій, особливо у сфері блокчейну [87]. Цей принцип передбачає фокусування законодавства на функціональному призначенні та правових наслідках використання технологій, а не на їх технічних характеристиках. Аргументація на користь такого підходу включає наступні аспекти.

По-перше, технологічна нейтральність забезпечує довговічність правових норм в умовах швидкої технологічної еволюції. Як свідчить досвід регулювання електронної комерції та телекомунікацій, технологічно-специфічні норми швидко застарівають, потребуючи постійних змін до законодавства, що створює правову невизначеність та підвищує регуляторні витрати. Навпаки, технологічно нейтральні норми залишаються ефективними протягом тривалого часу, незалежно від зміни технологічних стандартів [97].

По-друге, нейтральний підхід створює рівні конкурентні умови для різних технологічних рішень, запобігаючи дискримінації нових технологій. Емпіричні дослідження регуляторних режимів у різних юрисдикціях демонструють, що технологічно-специфічне регулювання часто створює необґрунтовані бар'єри для нових учасників ринку та стримує інновації [19].

По-третє, у контексті блокчейну, які характеризуються особливо високою швидкістю інновацій та різноманітністю реалізацій, технологічна нейтральність

набуває критичного значення. Як було встановлено в Розділі 1, блокчейн трансформує інформаційні відносини, що призводить до постійної появи нових форм взаємодії (DeFi, DAO, NFT). Регулювання, прив'язане до технічних рішень, створюватиме регуляторні прогалини для нових форм блокчейн-застосувань [139].

Хоча перші кроки до регулювання блокчейн-технологій були здійснені з прийняттям ЗУ "Про віртуальні активи" [102], цей акт лише частково відповідає вимогам технологічної нейтральності, не охоплюючи новітні форми блокчейн-відносин. Принцип технологічної нейтральності у блокчейн-регулюванні реалізується на трьох рівнях: базовому (відсутність прив'язки до технічних стандартів), функціональному (регулювання за функціональними ознаками) та цільовому (фокус на цілях регулювання). При цьому важливо зберігати баланс між нейтральністю та правовою визначеністю, оскільки абстрактність може ускладнювати правозастосування.

Для імплементації технологічної нейтральності в законодавство необхідно:

1. Внести зміни до ЗУ "Про віртуальні активи" [102], розширивши дефініції відповідно до функціонального підходу;
2. оновити положення ЦКУ [7], включивши віртуальні активи до об'єктів цивільних прав;
3. розробити рамковий закон про блокчейн-технології, що встановлюватиме базові принципи регулювання;
4. гармонізувати законодавство з міжнародними стандартами.

Цей підхід створить середовище, що відповідатиме викликам і трансформаціям. Однак принцип технологічної нейтральності потребує доповнення іншим принципом – забезпеченням балансу між стимулюванням інновацій та захистом прав учасників.

Пошук оптимального балансу між стимулюванням інновацій та захистом прав учасників є фундаментальним завданням при вдосконаленні правового регулювання блокчейн-технологій. Цей баланс передбачає створення умов для розвитку інноваційних рішень. Водночас необхідно забезпечити належний захист прав та

інтересів усіх залучених суб'єктів. Теоретичне осмислення цього балансу вимагає аналізу трансформації поняття "публічний інтерес" у контексті блокчейн-технологій.

Як описано в Розділі 1.1, децентралізована архітектура блокчейну створює як нові можливості (прозорість, автоматизація зобов'язань), так і ризики (незворотність транзакцій, складність ідентифікації відповідальних суб'єктів) [3].

Для ефективного регулювання необхідно розуміти блокчейн не лише як технічну, але і як інституційну інновацію. Ця технологія трансформує сам механізм соціальної координації та довіри, впливаючи на базові умови суспільної взаємодії.

У такій парадигмі захист прав стає не обмеженням інновацій, а необхідною умовою їх сталого розвитку, створюючи інституційне середовище, що сприяє довірі до нових технологічних рішень. Водночас інновації формують нові механізми реалізації та захисту прав, які можуть бути ефективнішими за традиційні підходи.

У Розділі 2 було розглянуто приватно-правові аспекти блокчейн-відносин, зокрема специфіку правочинів, захисту прав власності та відповідальності у децентралізованому середовищі. Встановлено, що традиційні цивілістичні механізми потребують адаптації до особливостей блокчейну, особливо щодо смарт-контрактів та захисту прав на віртуальні активи [5, 79].

Міжнародний досвід (Розділ 3) демонструє різні підходи до балансування інновацій та захисту прав. У Сінгапурі застосовується ризик-орієнтований підхід з "регуляторними пісочницями" для інноваційних проєктів та чіткими вимогами щодо захисту споживачів, тоді як у США підхід SEC фокусується переважно на захисті інвесторів, іноді обмежуючи інновації заради безпеки ринку [17, 41].

Для України пошук балансу має враховувати національні особливості: високий рівень технологічної освіченості населення, значний потенціал IT-сектору, але недостатньо розвинену фінансову інфраструктуру та обмежені регуляторні ресурси [4, 8]. За таких умов необхідний комплексний підхід, що забезпечить сприятливе середовище для інновацій з одночасним захистом прав учасників.

Для досягнення оптимального балансу пропонується комплекс заходів:

1. Впровадження "регуляторних пісочниць" для тестування інноваційних блокчейн-рішень під наглядом регуляторів, але з обмеженими вимогами.

- Це потребує внесення змін до ЗУ "Про фінансові послуги та державне регулювання ринків фінансових послуг" [141] щодо експериментальних режимів для інноваційних фінансових сервісів.

2. Розробка підходу до регулювання з диференціацією вимог залежно від ризику.
   - Для проєктів, що працюють з інвесторами або зберігають значні суми, слід застосовувати жорсткіші вимоги щодо капіталізації та безпеки.
   - Для невеликих проєктів доцільно застосовувати спрощений режим.
3. Заохочення саморегулювання через асоціації учасників, що розроблятимуть:
   - стандарти та кодекси поведінки;
   - механізми вирішення спорів.
4. Впровадження основ захисту споживачів, адаптованих до специфіки блокчейн-технологій (детальні механізми розглядаються в підрозділі 4.2).
5. Розробка механізмів обов'язкового розкриття інформації для проєктів, що залучають кошти через токенізацію (ICO, IEO, STO) [48].
   - Необхідне внесення змін до профільних законів.
6. Створення ефективних механізмів вирішення блокчейн-спорів:
   - спеціалізовані процедури арбітражу;
   - визнання блокчейн-записів як доказів;
   - нові механізми вирішення спорів через зміни до процесуальних кодексів.

Методологічно пошук балансу між інноваціями та захистом прав учасників структурується через призму теорії регуляторного впливу, яка передбачає:

1. Ідентифікацію ризиків та вигод для різних категорій стейкхолдерів;
2. Оцінку ймовірності та масштабу цих ризиків і вигод;
3. Аналіз ефективності різних регуляторних інструментів;
4. Встановлення механізмів моніторингу та адаптації регулювання.

Застосування цієї методології забезпечує системний підхід, що дозволяє уникнути як надмірної зарегульованості, так і регуляторних прогалин.

Таким чином, досягнення балансу між стимулюванням інновацій та захистом прав учасників потребує системного підходу до вдосконалення законодавства. Запропоновані заходи спрямовані на створення правового середовища, що сприятиме розвитку блокчейн-технологій в Україні з одночасним забезпеченням належного захисту для всіх учасників ринку.

Розглянувши концептуальні основи регулювання, варто перейти до конкретних напрямків модернізації матеріально-правового регулювання, які втілюватимуть ці принципи на практиці.

Модернізація матеріально-правового регулювання блокчейн-технологій є невіддільною частиною вдосконалення правового поля України. Проведений у Розділі 2 аналіз приватно-правових аспектів блокчейн-відносин виявив особливості застосування методів приватно-правового регулювання (Розділ 2.1), трансформацію принципу автономії волі (Розділ 2.1), специфіку блокчейн-правочинів (Розділ 2.1), нові договірні механізми (Розділ 2.1) та особливості права власності на віртуальні активи (Розділ 2.2). На основі цього аналізу пропонується модернізація матеріально-правового регулювання, яка передбачає:

- адаптацію чинного законодавства до особливостей нових відносин;
- уточнення правового статусу віртуальних активів та смарт-контрактів;
- регулювання нових форм взаємодії;
- удосконалення механізмів оподаткування;
- розвиток систем захисту інтелектуальної власності;
- забезпечення інформаційної безпеки.

Теоретичні основи трансформації правових інститутів під впливом блокчейн-технологій детально досліджені в Розділі 2, зокрема в підрозділах 2.1 (методи регулювання та цивільно-правова природа блокчейн-правочинів) та 2.2 (право власності на віртуальні активи). На основі цього аналізу можна виділити ключові напрями трансформації:

1. Перехід до алгоритмічної довіри, що змінює принципи регулювання;

2. Переосмислення концепції правосуб'єктності;
3. Зміна сутності договорів через їх автоматизоване виконання;
4. Трансформація правомочностей власника у цифровому середовищі.

Реалізація матеріально-правових змін неможлива без відповідних інституційно-правових механізмів, які забезпечать їх впровадження та функціонування.

Визначення правового статусу віртуальних активів та смарт-контрактів є фундаментальним завданням для інтеграції блокчейн-технологій. Наразі правовий режим цих об'єктів, детально проаналізованих у Розділі 1.2, залишається недостатньо врегульованим, що створює невизначеність для учасників ринку.

ЗУ "Про віртуальні активи" [102] визначив віртуальні активи як нематеріальні блага. Для вдосконалення їх правового статусу пропонується:

1. Запровадити функціональну класифікацію віртуальних активів за міжнародними стандартами (як описано в Розділі 3.1):
   - платіжні (криптовалюти);
   - інвестиційні (токенізовані цінні папери);
   - утилітарні (доступ до сервісів);
   - гібридні.
2. Впровадити диференційований правовий режим для кожної категорії з відповідним нормативним регулюванням.
3. Внести зміни до ЦКУ [7], включивши їх до переліку об'єктів цивільних прав.
4. Визначити володіння ключами як форму володіння віртуальними активами.

Щодо правового статусу смарт-контрактів, фундаментальна проблематика яких розкрита в Розділі 2.1, наразі вони залишаються юридично невизначеними.

На основі дуалістичної природи смарт-контрактів як форми фіксації домовленостей (Розділ 2.1) та програмного коду (Розділ 1.2), для імплементації цього розуміння в українське законодавство пропонується:

- Зміни до ЦКУ [7]:
  - Доповнити ст. 639 щодо укладення договору у формі смарт-контракту;

- Змінити ст. 205, визначивши їх як форму електронного правочину;
- Додати в ст. 526 положення про автоматизоване виконання зобов'язань.

Перспективним напрямом є інтеграція блокчейн-систем з державними реєстрами для автоматизації реєстрації переходу прав.

Таким чином, удосконалення правового статусу віртуальних активів та смарт-контрактів є комплексним завданням, що потребує системних змін до законодавства. Запропоновані заходи створять правову визначеність для учасників ринку, сприятимуть інтеграції блокчейн-технологій у господарську діяльність та забезпечать належний захист прав у цифровому середовищі.

На основі аналізу унікальних форм організації та взаємодії в блокчейн-середовищі, проведеного в Розділах 2.1 (щодо принципу автономії волі) та 2.3.2 (щодо класифікації договорів), а також з урахуванням міжнародного досвіду (Розділ 3.2), пропонуються такі підходи до регулювання нових форм блокчейн-відносин:

1. Для DAO, враховуючи їх унікальні механізми децентралізованого прийняття рішень та автоматизованого виконання правил, пропонується:
   - Розробити спеціальний закон про DAO; або
   - Внести зміни до ЗУ "Про товариства з обмеженою та додатковою відповідальністю" [142], доповнивши його розділом про "Децентралізовані автономні організації" (ДАО) як особливу форму Товариства з обмеженою відповідальністю.
2. Встановити мінімальні вимоги для реєстрації DAO:
   - Обов'язкова публікація White Paper;
   - Проведення аудиту смарт-контрактів з отриманням сертифіката;
   - Обрання шляхом децентралізованого голосування щонайменше одного фізичного або юридичного представника для юридичної взаємодії з третіми особами (компромісне рішення для забезпечення взаємодії з традиційною правовою системою);
   - Внесення мінімального початкового капіталу.
3. Запровадити спеціальні механізми захисту прав учасників та кредиторів:

- Обов'язкова публікація протоколів голосування та фінансової звітності;
- Створення резервного фонду для компенсації збитків від помилок;
- Механізм "оракулів" для введення інформації в смарт-контракти;
- Спеціальні процедури вирішення спорів між учасниками.

4. Передбачити перехідний період (2 роки) для DAO, зареєстрованих в інших юрисдикціях, з можливістю спрощеної реєстрації та податковими стимулами.

Необхідно також визначити механізми захисту прав учасників DAO, врегулювати питання відповідальності, встановити правила ліквідації та розподілу залишкових активів, а також процедури вирішення патових ситуацій у голосуванні.

Як показано в Розділі 3, регулювання DeFi є складним завданням. Ця складність обумовлена відсутністю централізованого суб'єкта, що підлягає нагляду [18, 132].

Для адаптації українського законодавства до специфіки DeFi пропонується внести зміни до ЗУ "Про фінансові послуги та державне регулювання ринків фінансових послуг" [141], які б визначали особливості надання фінансових послуг через децентралізовані протоколи. Важливо встановити вимоги до розробників та операторів DeFi-протоколів щодо розкриття інформації про ризики, аудиту смарт-контрактів та механізмів захисту від маніпуляцій, а також розробити механізми моніторингу на предмет відповідності AML [99]. Необхідно також визначити особливості оподаткування доходів від участі в DeFi-протоколах.

Як показано в Розділі 3, правовий статус NFT залишається невизначеним у багатьох юрисдикціях, що створює невизначеність щодо прав власності та інтелектуальної власності на такі активи.

Для врегулювання статусу NFT пропонується внести зміни до ЗУ "Про авторське право і суміжні права" [143]. Важливо чітко розмежувати право власності на NFT як цифровий актив та авторські права на твір, який цей токен представляє, визначивши, що володіння NFT за замовчуванням надає лише право на особисте некомерційне використання об'єкта, якщо інше не передбачено в умовах продажу.

Необхідно також внести зміни до ПКУ [144] щодо оподаткування операцій з NFT (прибутку від продажу та роялті) та встановити правила визначення ринкової вартості

NFT для цілей оподаткування. Для забезпечення прозорості ринку NFT доцільно розробити вимоги до маркетплейсів щодо перевірки автентичності творів, розкриття інформації про права, що передаються з NFT, та механізмів вирішення спорів.

Таким чином, регулювання нових форм блокчейн-відносин потребує підходу, який враховує їхню специфіку та забезпечує баланс між інноваційністю та захистом прав учасників. Запропоновані заходи створять правову визначеність щодо статусу та функціонування цих нових форм, сприятимуть їх інтеграції в правове поле України та забезпечать належний рівень захисту прав учасників.

Теоретичний аналіз нових форм блокчейн-відносин виявляє концептуальні виклики та дозволяє розробити уніфіковані методологічні підходи до їх вирішення. Ключовою особливістю цих форм є їх гібридна природа, що поєднує технологічні, економічні та правові аспекти, які не вкладаються у традиційні регуляторні категорії. Методологічно доцільним є застосування функціонального підходу, що фокусується на економічній сутності та суспільному впливі, незалежно від технічної реалізації, забезпечуючи регуляторну гнучкість при збереженні захисту суспільних інтересів.

Концептуально регулювання нових форм блокчейн-відносин має будуватися на трьох фундаментальних принципах:

1. Функціональній еквівалентності, що передбачає аналогічне регулювання для функціонально ідентичних послуг;
2. Пропорційності регуляторного втручання відповідно до рівня ризику;
3. Технологічній нейтральності, що дозволяє застосовувати регуляторні вимоги до різних технологічних реалізацій [87, 97].

Ці принципи створюють методологічну основу для регуляторних рішень, здатних адаптуватися до еволюції блокчейн-технологій.

Питання оподаткування операцій з віртуальними активами є одним з ключових аспектів правового регулювання блокчейн-технологій. Цей аспект безпосередньо впливає на економічну ефективність та інвестиційну привабливість галузі. Наразі в Україні відсутній чіткий режим оподаткування таких операцій. Це створює правову невизначеність для учасників ринку та ускладнює адміністрування податків.

Як було визначено в Розділі 1, віртуальні активи характеризуються особливими властивостями, що створює специфічні виклики для системи оподаткування. Аналіз міжнародного досвіду (Розділ 3) демонструє різноманітність підходів: від застосування загальних правил оподаткування майна чи фінансових інструментів до розробки спеціальних податкових режимів для криптоактивів.

Пропонується розробити підхід до оподаткування операцій з віртуальними активами, який би враховував як інтереси держави, так і необхідність стимулювання інноваційних технологій. Для цього необхідно внести зміни до ПКУ [144] щодо:

1. Оподаткування доходів фізичних осіб:
   - встановити пільгову ставку ПДФО для інвестиційного прибутку від операцій з віртуальними активами на рівні 5% на початковому етапі;
   - передбачити поступове підвищення до стандартних 18% протягом 5 років
   - стимулювати декларування таких доходів.
2. Оподаткування прибутку підприємств:
   - застосовувати стандартну ставку податку на прибуток (18%);
   - для стартапів, які розробляють блокчейн-рішення, передбачити податкові канікули на період до 3 років з моменту реєстрації.
3. Оподаткування майнінгу та стейкінгу криптовалют:
   - розглядати доходи від майнінгу як підприємницьку діяльність;
   - застосування спрощеної системи для індивідуальних майнерів;
   - для стейкінгу режим, аналогічний оподаткуванню пасивних доходів.
4. Механізми оцінки вартості віртуальних активів:
   - визначати вартість на основі ринкових курсів на визнаних криптобіржах;
   - розробити механізми оцінки через спеціалізовані сервіси;
   - встановити особливі правила для унікальних активів, таких як NFT.
5. Механізми адміністрування податків:
   - впровадити систему електронного декларування операцій;
   - забезпечити механізми обміну інформацією з криптобіржами;
   - створити зрозумілі інструкції для платників податків.

Важливим аспектом є впровадження механізмів запобігання подвійному оподаткуванню, особливо для транскордонних операцій, через внесення відповідних положень до міжнародних податкових угод. Доцільно також розробити механізми податкового стимулювання для проєктів, які використовують блокчейн-технології для вирішення суспільно важливих завдань (у сфері охорони здоров'я, освіти, державного управління) через податкові пільги, прискорену амортизацію тощо.

Для ефективного адміністрування податків необхідно розробити методичні рекомендації для податкових органів щодо перевірки операцій та провести навчання співробітників податкової служби з питань блокчейн-технологій та криптографії.

Таким чином, такі зміни створять прозорий режим оподаткування операцій з віртуальними активами, сприяючи виходу цієї сфери з тіньового сектора, збільшенню податкових надходжень та стимулюванню розвитку технологій.

Поряд із фіскальними аспектами, не менш важливим напрямом удосконалення правового регулювання є захист інтелектуальної власності, особливо з огляду на більшу роль блокчейну у створенні та обігу цифрових об'єктів авторського права.

Захист інтелектуальної власності в контексті блокчейн-технологій є перспективним напрямом удосконалення правового регулювання. Цей напрям має значний потенціал для підвищення ефективності захисту авторських прав, патентів, торгівельних марок та інших об'єктів інтелектуальної власності. Водночас специфіка блокчейн-середовища створює нові виклики для традиційних механізмів захисту. Це вимагає розробки нових теоретичних підходів та їх практичної імплементації.

Традиційна теорія фіксації авторства базується на презумпції авторства та системі державної реєстрації (Бернська конвенція, ст. 15) [116]. Блокчейн з його функцією незмінного часового штампа створює технологічну можливість для правдивої фіксації пріоритету без централізованого реєстратора [95]. З огляду на це слід доповнити ст. 11 ЗУ "Про авторське право і суміжні права" [143] положенням: "Фіксація твору в блокчейн-реєстрі з використанням електронного підпису автора створює презумпцію авторства, якщо не доведено інше".

Теорія програмованих прав [87] передбачає можливість автоматизованого ліцензування та захисту прав через смарт-контракти. Це трансформує традиційне

розуміння ліцензійних відносин як договірних у бік технологічно-самовиконуваних. З огляду на це слід внести зміни до ст. 1109 ЦКУ [7] "Ліцензійний договір", доповнивши її положенням: "Ліцензійний договір може укладатися у формі смарт-контракту, що автоматично забезпечує виконання його умов, включаючи відрахування роялті".

Концепція розмежування права власності на NFT та авторські права на твір, представлений цим токеном, базується на теорії функціонального розмежування різних типів прав [121] і потребує чіткого законодавчого закріплення, а саме слід доповнити ЗУ "Про віртуальні активи" [102] статтею "Невзаємозамінні токени", із зазначенням: "Набуття права власності на невзаємозамінний токен не означає автоматичного набуття авторських прав на твір, представлений цим токеном, якщо інше прямо не передбачено умовами придбання".

Теорія технологічно-підтримуваного захисту прав [149] передбачає використання технологічної інфраструктури для автоматичного виявлення та запобігання порушенням. Це є розвитком традиційної теорії технічних засобів захисту авторських прав. Відповідно буде доречно внести зміни до ст. 52 Закону "Про авторське право і суміжні права" [143], додавши положення про обов'язок маркетплейсів NFT "впроваджувати системи автоматичної перевірки наявності прав на токенізовані об'єкти інтелектуальної власності та блокування несанкціонованого використання".

Як показано в Розділі 1 та деталізовано в Розділі 2.1, блокчейн характеризується незмінністю записів, децентралізованим характером та можливістю автоматизації правил за допомогою смарт-контрактів. Аналіз у Розділі 2.1 виявив специфічні механізми забезпечення виконання зобов'язань у блокчейн-середовищі, які можуть бути ефективно використані для захисту прав інтелектуальної власності: для фіксації пріоритету створення творів, автоматизації ліцензування та розподілу роялті, а також для запобігання неавторизованому використанню.

Для адаптації українського законодавства до використання блокчейн-технологій у сфері захисту інтелектуальної власності пропонується:

1. Авторське право:

- Внести зміни до ЗУ "Про авторське право і суміжні права" [143], які б визнали блокчейн-записи як доказ авторства та пріоритету створення.
- Встановити, що фіксація твору в блокчейн-реєстрі з використанням електронного підпису автора створює презумпцію авторства, що спростить процес доказування та зменшить кількість спорів.

2. Патентне право:
   - Внести зміни до ЗУ "Про охорону прав на винаходи і корисні моделі" [145] для використання блокчейну при фіксації пріоритету патентних заявок.
   - Забезпечити публікацію відомостей про патентні заявки в блокчейні, що підвищить прозорість патентної системи.
3. Торгівельні марки:
   - Внести зміни до ЗУ "Про охорону прав на знаки для товарів і послуг" [146] щодо використання блокчейну для реєстрації торгівельних марок.
   - Впровадити механізми відстежування використання торгівельних марок, що допоможе в боротьбі з контрафактною продукцією.
4. Смарт-контракти в ліцензуванні:
   - Розробити правову базу для використання смарт-контрактів у ліцензуванні об'єктів інтелектуальної власності.
   - Визначити юридичну силу смарт-контрактів для передачі прав, нарахування роялті та обмеження використання творів.
5. Регулювання NFT:
   - Створити механізми для захисту прав в контексті NFT.
   - Чітко розмежувати право власності на NFT та авторські права на твір.
   - Встановити вимоги щодо перевірки прав на твори, що токенізуються.
6. Державний реєстр:
   - Створення блокчейн-реєстру об'єктів інтелектуальної власності.
   - Забезпечити інтеграцію з чинними реєстрами.
   - Засіб для фіксації авторства, реєстрації патентів та торгівельних марок.

7. Вирішення спорів
    - Запровадити арбітражні процедури та онлайн-механізми для випадків: порушення авторських прав при створенні NFT; спорів щодо смарт-контрактів; та конфліктів між правовласниками.

Важливим аспектом є саморегулювання через галузеві стандарти та кодекси етики для платформ, які використовують блокчейн для захисту інтелектуальної власності, встановлюючи вимоги до прозорості, захисту та використання творів.

Таким чином, удосконалення регулювання захисту інтелектуальної власності в блокчейні створить нові можливості для правовласників, підвищить прозорість системи захисту прав та сприятиме розвитку креативних індустрій в Україні.

Хоча захист інтелектуальної власності є важливим аспектом правового регулювання блокчейн-технологій, не менш значущим є питання загальної адаптації інформаційного законодавства до нових технологічних реалій.

Використання блокчейн-технологій зумовлює необхідність адаптації інформаційного законодавства до нових реалій. Ключовими аспектами, які потребують удосконалення, є: захист персональних даних; електронна ідентифікація; інформаційна безпека та доступ до інформації в блокчейн-системах.

Специфічні інформаційні відносини в блокчейні (Розділ 1.1) потребують адаптації традиційних принципів інформаційного права.

Пропонується внести зміни до ЗУ "Про захист персональних даних" [147], які б:

1. Визначали особливості обробки персональних даних у блокчейні, включаючи ролі та відповідальність учасників: розробників; валідаторів та користувачів.
2. Встановлювали механізми реалізації прав суб'єктів даних, включаючи альтернативні підходи до видалення даних:
    - криптографічне шифрування ключів доступу;
    - зберігання чутливих даних поза блокчейном.
3. Визначали особливості транскордонної передачі персональних даних.
4. Запроваджували ризик-орієнтований підхід до оцінки впливу на захист даних.

Другий важливий аспект – розвиток системи електронної ідентифікації та довірчих послуг. Блокчейн може стати технологічною основою для децентралізованих систем ідентифікації, які підвищують безпеку та приватність [89]. Для цього пропонується внести зміни до ЗУ "Про електронні довірчі послуги" [148], які б:

- Визнавали можливість використання блокчейну для надання довірчих послуг (створення та перевірка електронних підписів, печаток та міток часу);
- Встановили вимоги до блокчейн-систем щодо безпеки, доступності та аудиту;
- Визначали статус децентралізованих ідентифікаторів;
- Регулювали використання концепції самосуверенної ідентичності.

Третій аспект – адаптація законодавства про інформаційну безпеку. Блокчейн-системи мають як переваги (стійкість до маніпуляцій, розподілене зберігання), так і вразливості (атаки 51%, помилки) [20, 46]. Для підвищення безпеки пропонується внести зміни до ЗУ "Про основні засади забезпечення кібербезпеки України" [150] щодо:

- Особливостей забезпечення кібербезпеки блокчейн-систем;
- Вимог до аудиту безпеки блокчейн-платформ та смарт-контрактів;
- Реагування на інциденти в блокчейн-системах;
- Управління ризиками, пов'язаними з використанням блокчейн-технологій.

Четвертий аспект – регулювання доступу до інформації та прозорості блокчейн-систем. Для цього пропонується внести зміни до ЗУ "Про доступ до публічної інформації" [151], які б визначали особливості доступу до інформації в публічних блокчейнах, встановлювали вимоги до прозорості систем, що використовуються для надання публічних послуг, та регулювали баланс між прозорістю та конфіденційністю, особливо для систем з чутливою інформацією.

П'ятий аспект – адаптація законодавства про електронну комерцію та електронні документи. Пропонується внести зміни до ЗУ "Про електронну комерцію" [152] та ЗУ "Про електронні документи та електронний документообіг" [153], які б визнавали

юридичну силу смарт-контрактів як особливої форми електронних правочинів, встановлювали вимоги до документів, що зберігаються в блокчейні, та регулювали використання блокчейну для автоматизації бізнес-процесів.

Таким чином, адаптація інформаційного законодавства до викликів блокчейн-технологій потребує системного підходу з урахуванням технічних особливостей та балансу інтересів різних сторін. Запропоновані зміни створять правову визначеність використання блокчейну в інформаційних відносинах, підвищать рівень захисту даних та інформаційної безпеки, а також сприятимуть розвитку інноваційних рішень.

З урахуванням аналізу приватно-правових відносин у Розділі 2, особливо аспектів методів регулювання та автономії волі, можна визначити ключові напрями трансформації інформаційно-правових відносин:

1. Регулювання через технологію, де код стає регулятором поведінки учасників.
2. Технологічна адекватність як доповнення до технологічної нейтральності.
3. Багаторівнева модель приватності замість бінарної моделі.
4. Еволюція від централізованої до криптоекономічної безпеки.

Ці положення формують основу для подальшого розвитку інформаційного законодавства в умовах поширення блокчейн-технологій та можуть бути використані для вдосконалення підходів не лише в Україні, але й на міжнародному рівні.

4.2. Інституційно-правові механізми та захист прав учасників

Ефективне регулювання блокчейн-технологій неможливе без інституційних механізмів. Ці механізми забезпечують імплементацію норм та контроль за їх дотриманням. Удосконалення цих механізмів є важливим аспектом для створення сприятливого середовища розвитку блокчейн-технологій в Україні.

Регулювання блокчейн-технологій в Україні наразі розподілено між кількома органами: НБУ, НКЦПФР та Мінцифри. Така розпорошеність створює ризики дублювання функцій, неузгодженості та регуляторної невизначеності.

Враховуючи обмеженість ресурсів та необхідність ефективного використання інституційного потенціалу, пропонується оптимізація регуляторів шляхом розмежування їхніх повноважень та забезпечення координації діяльності.

Необхідним є внесення змін до ЗУ "Про віртуальні активи" [102] та інших НПА для визначення компетенції регуляторів та створення координаційних механізмів.

Пропонується такий розподіл регуляторних функцій:

- НБУ:
  - Регулювання платіжних віртуальних активів;
  - Нагляд за відповідністю операцій вимогам валютного законодавства;
  - Контроль за інтеграцією віртуальних активів у платіжні системи;
  - Моніторинг впливу віртуальних активів на фінансову стабільність.
- НКЦПФР:
  - Регулювання інвестиційних віртуальних активів;
  - Нагляд за діяльністю торгових платформ та бірж віртуальних активів;
  - Захист прав інвесторів та вимоги до розкриття інформації;
  - Протидія маніпулюванню ринком та інсайдерській торгівлі.
- Мінцифри:
  - Формування загальної політики у сфері блокчейн-технологій;
  - Розробка технічних стандартів та сертифікація;
  - Ліцензування провайдерів послуг (крім фінансових);
  - Координація використання блокчейну в державному секторі.

Обґрунтування запропонованого розподілу повноважень базується на теорії інституційного дизайну [155, 156] та аналізі регуляторної ефективності.

Дослідження Quintyn & Taylor [157], що охоплювало 32 країни протягом 15-річного періоду, емпірично підтвердило, що ефективність інституційної архітектури залежить від трьох ключових факторів:

5. Чіткості розмежування компетенцій;
6. Наявності формалізованих механізмів координації та інформаційного обміну;

7. Інституційної спроможності регуляторів.

Емпіричний аналіз Lavrijssen & Ottow [158] виявив, що регуляторні системи з чітким функціональним розподілом повноважень та ефективними механізмами координації в середньому на 27% ефективніші у досягненні регуляторних цілей порівняно з моделями дублювання повноважень:

8. Чіткість розмежування компетенцій – забезпечує уникнення як регуляторних прогалин, так і дублювання функцій, що підвищує правову визначеність для учасників ринку та зменшує транзакційні витрати. Як показали дослідження [159, 160], невизначеність розподілу повноважень між регуляторами призводить до "регуляторного паралічу" або, навпаки, до надмірного регуляторного навантаження через мультиплікацію вимог.
9. Наявність формалізованих механізмів координації та інформаційного обміну – критично важлива для забезпечення системної узгодженості регуляторних підходів. Емпіричні дослідження фінансових ринків [161, 162] демонструють, що відсутність таких механізмів була однією з причин регуляторних провалів під час фінансової кризи 2008 року.
10. Інституційна спроможність регуляторів – включає наявність відповідних ресурсів, компетенцій та повноважень для ефективного виконання регуляторних функцій. Дослідження інституційного розвитку регуляторів у різних країнах [157, 163] свідчать про прямий зв'язок між інституційною спроможністю та якістю регулювання.

Порівняльний аналіз міжнародного досвіду, проведений у Розділі 3, виявляє три моделі інституційної організації регулювання блокчейн-технологій:

- Концентрована – єдиний регулятор, що має переваги в концентрації експертизи, але потребує значних ресурсів для створення;
- Функціональна – розподіл повноважень за сферами між регуляторами;
- Гібридна – координаційний орган та функціональний розподіл повноважень.

Зіставлення цих моделей з українським інституційним контекстом, зокрема з урахуванням чинної інституційної спроможності регуляторів, особливостей міжвідомчої взаємодії та обмеженості ресурсів, дозволяє обґрунтовано стверджувати, що гібридна модель з елементами функціональної є найбільш доцільною. Ця модель дозволяє використовувати наявну експертизу регуляторів у відповідних сферах (НБУ – у платіжних системах, НКЦПФР – в інвестиційній сфері), мінімізувати витрати на створення нових інституційних структур та забезпечити органічну інтеграцію регулювання віртуальних активів у чинну систему фінансового регулювання, водночас забезпечуючи координацію через спеціальний орган.

Для забезпечення такої координації діяльності регуляторів пропонується створити Міжвідомчу раду з питань регулювання блокчейн-технологій та віртуальних активів. До складу ради входитимуть:

- Представники державних органів:
  - НБУ;
  - НКЦПФР;
  - Мінцифри;
  - Міністерства фінансів;
  - Державної податкової служби;
  - Державної служби фінансового моніторингу.
- Представники недержавного сектору:
  - Учасники ринку віртуальних активів;
  - Експертне середовище.
- Функції ради включатимуть:
  - Координацію розробки та імплементації нормативно-правових актів;
  - Розв'язання питань міжвідомчої компетенції;
  - Моніторинг ефективності регуляторних заходів;
  - Участь у міжнародному співробітництві.

Доцільно також розробити механізм "єдиного вікна" для суб'єктів ринку віртуальних активів на базі Мінцифри, що спрощуватиме взаємодію з регуляторами через централізоване приймання документів, консультацій та координацію нагляду.

Для підвищення інституційної спроможності регуляторів необхідно:

- Забезпечити навчання персоналу щодо блокчейну, криптографії та інновацій;
- Створити спеціалізовані підрозділи в кожному регуляторному органі;
- Розробити методологічні рекомендації для інспекторів та аудиторів;
- Забезпечити технічну інфраструктуру для моніторингу блокчейн-транзакцій.

Для підвищення прозорості та передбачуваності пропонується:

- Публікувати роз'яснення щодо застосування законодавства у цій сфері;
- Проводити консультації перед прийняттям нових регуляторних рішень;
- Впровадити механізм регуляторних пісочниць під наглядом регуляторів;
- Забезпечити ефективний обмін інформацією між регуляторами.

Для міжнародної гармонізації підходів до регулювання важливо забезпечити участь України в міжнародних організаціях та ініціативах, таких як FATF [99] та Технічний комітет ISO/TC 307 з блокчейну [50].

Таким чином, оптимізація системи регуляторів та координація їхньої діяльності є важливою передумовою для ефективного регулювання блокчейн-технологій в Україні. Запропоновані заходи забезпечать розподіл повноважень, допоможуть уникнути дублювання функцій та регуляторних прогалин, підвищать інституційну спроможність регуляторів та гарантуватимуть прозорість регуляторної діяльності.

У децентралізованому середовищі блокчейну саморегулювання відіграє важливу роль, забезпечуючи адаптивність та експертизу. Як показує досвід (Розділ 3.3), ефективність саморегулювання досягається поєднанням трьох підходів:

1. Ринкового (базується на конкуренції та репутації)
2. Інституційного (через формальні галузеві асоціації)
3. Мережевого (через децентралізовані механізми консенсусу)

Для України доцільно впровадити модель інституційного саморегулювання з елементами мережевого, що найкраще відповідає архітектурі блокчейн-систем.

Для ефективної імплементації моделі саморегулювання в Україні пропонуються такі конкретні заходи:

4. Законодавче закріплення статусу СРО у сфері блокчейн-технологій:
   - Внести зміни до ЗУ "Про віртуальні активи" [102], додавши розділ "Саморегулювання ринку віртуальних активів";
   - Встановити критерії визнання СРО: мінімальна кількість учасників (не менше 25% від загальної кількості ліцензованих учасників ринку), наявність кодексу етики, механізми контролю за членами;
   - Визначити процедуру державного визнання СРО через реєстрацію у регуляторах (НБУ, НКЦПФР, Мінцифри).
5. Делегування регуляторних повноважень до СРО:
   - Дозволити встановлювати технічні стандарти;
   - Надати право здійснювати нагляд за дотриманням стандартів;
   - Визнати сертифікацію як елемент спрощеної процедури ліцензування.
6. Запровадження механізмів підзвітності та прозорості СРО:
   - Встановити вимоги до розкриття інформації про діяльність СРО;
   - Запровадити механізм апеляції рішень СРО до державних регуляторів;
   - Передбачити аудит діяльності СРО незалежними експертами.
7. Створення стимулів для участі в саморегулюванні:
   - Запровадити спрощені процедури ліцензування для членів СРО;
   - Передбачити менший обсяг звітності для членів визнаних СРО;
   - Надати членам СРО пріоритетний доступ до регуляторних пісочниць;
8. Розробка механізмів координації між СРО та державними регуляторами:
   - Створити Раду з координації саморегулювання при Міжвідомчій раді;
   - Запровадити консультації з питань розробки нормативно-правових актів;
   - Визначити порядок спільного реагування на нові виклики ринку.

Реалізація цих заходів дозволить створити в Україні систему співрегулювання, що поєднує переваги саморегулювання з перевагами державного регулювання.

Саморегулювання є важливим елементом системи регулювання блокчейн-технологій, який доповнює державне регулювання та забезпечує більш гнучкий підхід до швидкозмінного технологічного середовища. Міжнародний досвід, проаналізований у Розділі 3.3, демонструє високу ефективність саморегулювання в юрисдикціях з розвиненими ринками криптоактивів.

Для України розвиток саморегулювання ринку блокчейн-технологій особливо актуальний з огляду на обмежені ресурси регуляторів та динамічний характер змін. Таке саморегулювання може ефективно доповнювати державне регулювання, забезпечуючи баланс між захистом публічних інтересів та стимулюванням інновацій.

Для розвитку саморегулювання пропонується внести зміни до ЗУ "Про віртуальні активи" [102], які б визначали правовий статус (СРО) у сфері блокчейн-технологій, їхні права та обов'язки, а також механізми взаємодії з регуляторами.

СРО у сфері блокчейн-технологій можуть виконувати такі функції:

- Розробка та впровадження стандартів для учасників ринку, включаючи кодекси етики, стандарти, вимоги до розкриття інформації та захисту споживачів;
- Проведення незалежного аудиту та сертифікації;
- Моніторинг ринку та виявлення ризиків, включаючи ознаки шахрайства та маніпулювання, з використанням спеціалізованих систем аналізу транзакцій;
- Освіта та підвищення обізнаності споживачів щодо безпечного використання блокчейн-технологій та ризиків інвестування в криптоактиви;
- Вирішення спорів між учасниками;
- Представництво інтересів галузі у взаємодії з державними органами.

Для ефективного функціонування саморегулювання необхідно визначити механізми взаємодії між СРО та державними регуляторами. Пропонується модель "співрегулювання", де держава встановлює загальні вимоги та контролює діяльність СРО, а СРО розробляють детальні стандарти та здійснюють нагляд за своїми членами.

Така модель може передбачати:

- Делегування СРО певних регуляторних функцій (реєстрація учасників ринку, перевірка відповідності вимогам, моніторинг дотримання стандартів);
- Визнання стандартів, розроблених СРО, як частини регуляторної бази;
- Проведення навчальних програм, досліджень та участь представників у роботі Міжвідомчої ради з питань регулювання блокчейн-технологій.

Важливим аспектом є забезпечення прозорості та підзвітності діяльності СРО через встановлення вимог до розкриття інформації про членство, стандарти, результати перевірок, а також регулярної звітності. Для стимулювання участі в саморегулюванні доцільно передбачити переваги для членів СРО, такі як спрощені процедури ліцензування або пріоритетний доступ до регуляторних пісочниць.

Таким чином, розвиток саморегулювання ринку блокчейн-технологій є важливим напрямом удосконалення інституційно-правових механізмів. Запропоновані заходи забезпечать більш гнучкий підхід до регулювання, підвищать довіру до галузі, захист споживачів та сприятимуть розвитку інновацій в Україні.

На основі аналізу, проведеного в Розділі 2 (захист права власності та цивільно-правовий захист), а також з урахуванням специфіки блокчейн-технологій, пропонується система заходів для вдосконалення захисту прав:

9. Захист права власності на віртуальні активи:
    - Внесення змін до ЦКУ [7];
    - Доповнення Закону "Про віртуальні активи" [102];
    - Створення цифрового депозитарію для фіксації прав.
10. Захист прав споживачів блокчейн-послуг:
    - Зміни до Закону "Про захист прав споживачів" [164];
    - Впровадження спеціалізованих процедур вирішення спорів;
    - Встановлення технічних вимог до провайдерів послуг;
    - Розробка механізмів компенсації збитків.

Важливим аспектом захисту прав споживачів є підвищення їхньої фінансової та технологічної грамотності. Пропонується розробити освітні програми та

інформаційні матеріали про блокчейн-технології, віртуальні активи та пов'язані з ними ризики, які можуть реалізовуватися Мінцифри, регуляторами та СРО.

Для ефективного захисту прав інвесторів у проєкти, що залучають кошти через продаж токенів (ICO, IEO, STO), пропонується встановити такі вимоги:

- Розкриття інформації про проєкт, його засновників, технічні особливості, бізнес-модель та плани розвитку у формі "білої книги";
- Проведення незалежного аудиту смарт-контрактів та технічної інфраструктури;
- Забезпечення прозорості використання коштів та регулярної звітності;
- Запровадження механізмів захисту інвесторів, таких як вимоги до ескроу-рахунків, поетапного фінансування або повернення коштів.

Таким чином, удосконалення механізмів захисту прав власності на віртуальні активи та прав споживачів блокчейн-послуг є важливим напрямом правового регулювання, що розвиває положення щодо балансу між інноваціями та захистом прав, розглянуті в підрозділі 4.1 Запропоновані заходи підвищать рівень довіри, забезпечать захист прав учасників та сприятимуть розвитку ринку в Україні.

Наукометричний аналіз ефективності різних механізмів захисту прав споживачів на ринках віртуальних активів демонструє, що найбільш дієвими є комплексні підходи, які поєднують:

11. вимоги до розкриття інформації;
12. пруденційні вимоги до постачальників послуг;
13. механізми компенсації збитків;
14. освітні ініціативи.

Дослідження показують, що оптимальним є ризик-орієнтований підхід, який передбачає пропорційність регуляторних вимог до рівня ризику, що створюється певною діяльністю, оскільки надмірне регулювання обмежує інновації, а недостатнє призводить до зловживань.

Професійні учасники ринку віртуальних активів відіграють ключову роль у функціонуванні екосистеми. До таких учасників належать:

- криптобіржі;
- кастодіальні сервіси;
- провайдери гаманців;
- торгівельні платформи.

Як встановлено в Розділі 3, міжнародний досвід демонструє тенденцію до посилення регулювання діяльності таких учасників. Це регулювання має на меті:

- запобігання зловживанням;
- забезпечення фінансової стабільності;
- захист прав споживачів.

ЗУ "Про віртуальні активи" [102] встановлює основи регулювання діяльності постачальників послуг, пов'язаних з віртуальними активами, однак багато аспектів їхньої діяльності залишаються недостатньо врегульованими. Для удосконалення регулювання пропонується розробити систему вимог до різних категорій професійних учасників, яка враховуватиме їхню роль, ризики та стандарти.

1. Для криптобірж та торгівельних платформ:
    - Ліцензування діяльності з різними категоріями ліцензій залежно від обсягів та цільової аудиторії;
    - Вимоги до мінімального капіталу та фінансової стійкості;
    - Сегрегація активів клієнтів та зберігання у холодних гаманцях;
    - Аудит безпеки та механізми запобігання маніпулюванню ринком;
    - Прозорість торгів та розкриття інформації.
2. Для кастодіальних сервісів:
    - Ліцензування з диференціацією вимог залежно від обсягів активів;
    - Вимоги до безпеки зберігання;
    - Обов'язкове страхування активів клієнтів;
    - Резервування та періодичне підтвердження наявності активів;
    - Ідентифікація клієнтів та верифікація транзакцій.

3. Для провайдерів гаманців та інфраструктурних сервісів:
    - Реєстрація діяльності;
    - Базові стандарти безпеки та захисту даних клієнтів;
    - Розкриття інформації про ризики.
4. Для DeFi-платформ та децентралізованих бірж:
    - Ризик-орієнтований підхід залежно від рівня децентралізації;
    - Вимоги до аудиту смарт-контрактів;
    - Розкриття інформації про ризики;
    - Сприяння розвитку децентралізованих механізмів управління ризиками.

Для всіх категорій професійних учасників важливим є встановлення вимог щодо AML/KYC відповідно до рекомендацій FATF [99]:

- KYC з урахуванням ризик-орієнтованого підходу;
- Моніторинг транзакцій та виявлення підозрілих операцій;
- Реалізація "правила подорожі", яке вимагає обміну інформацією про відправника та отримувача транзакцій між провайдерами послуг;
- Зберігання інформації про транзакції та клієнтів протягом певного періоду.

Реалізація цих пропозицій вимагає змін до ЗУ "Про віртуальні активи" [102] та розробки підзаконних НПА, а також гармонізації законодавства з міжнародними стандартами, зокрема з рекомендаціями FATF [99] та регламентом MiCA [68] в ЄС.

Таким чином, удосконалення регулювання діяльності професійних учасників ринку віртуальних активів є важливим напрямом розвитку правового регулювання блокчейн-технологій в Україні. Запропоновані заходи спрямовані на:

- - підвищення рівня захисту прав споживачів;
- - забезпечення фінансової стабільності;
- - створення прозорих правил для ведення бізнесу в цій сфері.

Методологічно регулювання діяльності професійних учасників ринку віртуальних активів має ґрунтуватися на синтезі трьох теоретичних підходів:

1. Теорії регульованого ринку [165], яка визнає необхідність державного втручання для подолання інформаційної асиметрії та захисту прав споживачів. У контексті блокчейн-технологій ця теорія обґрунтовує регулювання криптобірж та кастодіальних сервісів, де існує значна асиметрія інформації між професійними учасниками та споживачами.
2. Теорії інституційної економіки [158, 166], яка аналізує витрати та механізми ефективності ринкових взаємодій. Вона пояснює роль формальних та неформальних інститутів у забезпеченні функціонування ринку віртуальних активів та обґрунтовує необхідність розвитку саморегулювання та стандартів.
3. Теорії адаптивного регулювання [167], яка визнає необхідність гнучких регуляторних підходів у контексті технологічних інновацій. Ця теорія особливо релевантна для блокчейн-технологій, що швидко еволюціонують, і обґрунтовує використання експериментальних режимів та ризик-орієнтованого підходу.

Інтеграція цих підходів дозволяє розробити концептуальну основу для регулювання, що забезпечує баланс між ринковою ефективністю, захистом прав учасників, фінансовою стабільністю та технологічними інноваціями.

Проведений аналіз регулювання професійних учасників ринку віртуальних активів дозволяє сформулювати кілька ключових теоретичних положень, що розвивають чинні доктрини фінансового регулювання:

1. Концепція "розсередженої відповідальності" модифікує традиційну теорію фідуціарних обов'язків у контексті децентралізованих фінансів. На відміну від класичної моделі, де відповідальність концентрується у централізованих інституціях, у блокчейн-середовищі відповідальність розподіляється між різними учасниками екосистеми (розробниками протоколів, валідаторами, користувачами) пропорційно до їх ролі та впливу на функціонування системи. Ця концепція вимагає диференційованого підходу до регулювання різних категорій учасників з урахуванням їх фактичної ролі в екосистемі.
2. Теорія "регуляторних інваріантів" подолає дихотомію між функціональним (same activity, same regulation) та сутнісним (same risks, same regulation)

підходами до регулювання, поєднуючи їх елементи. Вона визначає базові регуляторні принципи (інваріанти), що застосовуються незалежно від технологічної реалізації, але допускає варіативність конкретних механізмів імплементації залежно від технологічної специфіки. Такий підхід забезпечує баланс між послідовністю регулювання та його адаптивністю до інновацій.

3. Парадигма "вбудованого регулювання" трансформує традиційну модель зовнішнього нагляду у бік інтеграції регуляторних механізмів у саму архітектуру технологічних систем. У контексті блокчейну це означає можливість програмування регуляторних вимог безпосередньо в протоколи та смарт-контракти, що забезпечує автоматичне дотримання правил та зменшує витрати на контроль. Ця парадигма узгоджується з концепцією "регуляторних технологій" (RegTech), але розширює її, розглядаючи архітектуру технології як невіддільний елемент регуляторної системи.

Ці теоретичні положення формують фундамент для розробки нової парадигми регулювання децентралізованих фінансових систем, яка враховує їх принципово нову архітектуру та механізми функціонування. Вони можуть бути використані не лише для вдосконалення регулювання блокчейн-технологій, але й для переосмислення традиційних підходів до фінансового регулювання в умовах цифрової економіки.

Після розгляду регулювання діяльності учасників, перейдемо до процесуальних та інфраструктурних аспектів, які забезпечують реалізацію матеріальних норм.

4.3. Процесуальні аспекти та імплементація регулювання

На основі аналізу процесуальних аспектів, розглянутих у Розділі 2.2 (особливості доказування), необхідно визнати, що традиційні механізми вирішення спорів не повністю відповідають специфіці блокчейн-технологій через:

- децентралізований характер;
- транскордонність операцій;
- анонімність учасників;
- незворотність транзакцій;

- складність технічної експертизи.

Для ефективного вирішення блокчейн-спорів та визначення юрисдикції необхідно переосмислити три ключові концепції:

1. Юрисдикції через транскордонність;
2. Доказування через визнання особливого статусу криптографічних доказів;
3. Виконання рішень – через впровадження "технологічного примусу".

Для імплементації цих концепцій пропонуються такі конкретні зміни:

1. Зміни до процесуальних кодексів щодо юрисдикції:
   - Доповнити ст. 26 Цивільного процесуального кодексу України [168] положеннями про розгляд спорів, пов'язаних з віртуальними активами;
   - Встановити критерії визначення підсудності блокчейн-спорів: місцезнаходження постачальника послуг, власника віртуальних активів, місце виконання смарт-контрактів чи розміщення вузлів або валідаторів;
   - Передбачити механізми вирішення конфліктів юрисдикцій через міжнародне судове співробітництво.
2. Зміни щодо доказової сили блокчейн-записів:
   - Внести зміни до ст. 100 Цивільного процесуального кодексу України [171], ст. 96 Господарського процесуального кодексу України [169] та ст. 99 Кодексу адміністративного судочинства України [170], визначивши блокчейн-записи як особливий вид електронних доказів;
   - Встановити критерії оцінки достовірності блокчейн-записів;
   - Розробити стандарти фіксації, збору та зберігання блокчейн-доказів;
   - Визначити порядок залучення експертів для верифікації записів.
3. Практичні механізми виконання рішень:
   - Доповнити ЗУ "Про виконавче провадження" [171] положеннями щодо звернення стягнення на віртуальні активи;
   - Запровадити інститут "цифрового депозитарію" для зберігання віртуальних активів під час судового процесу;

- Встановити порядок передачі приватних ключів або доступу до гаманців;
- Розробити механізми співробітництва для виконання рішень.

4. Створення спеціалізованих інституцій:
   - Сформувати спеціалізовані судові колегії з розгляду блокчейн-спорів при господарських судах обласного рівня;
   - Створити Центр технічної експертизи блокчейн-доказів при Науково-дослідному інституті судових експертиз;
   - Забезпечити навчання суддів та судових експертів щодо блокчейну.

Реалізація цих рекомендацій дозволить створити систему вирішення блокчейн-спорів, що забезпечить правову визначеність та сприятиме розвитку індустрії.

Розвиток інфраструктури ринку віртуальних активів є необхідною умовою для ефективного функціонування блокчейн-екосистеми та інтеграції віртуальних активів у економіку. Як визначено в Розділі 1, блокчейн-технології потребують специфічної інфраструктури для забезпечення надійності, безпеки та доступності сервісів.

Розробка пропозицій щодо вдосконалення інфраструктури ґрунтується на чіткій теоретичній основі, що забезпечує їхню системність та ефективність.

Згідно з теорією фінансової архітектури [172], ефективний ринок потребує інтегрованої багаторівневої інфраструктури, що включає:

- торгівельні майданчики;
- розрахунково-клірингові механізми;
- системи зберігання активів;
- інформаційно-аналітичні сервіси.

Особливістю блокчейну є конвергенція цих рівнів в єдиній технологічній екосистемі. З огляду на це виникають пропозиції:

- Прийняти Концепцію розвитку ринку віртуальних активів на 2027-2030 роки;
- Запровадити ліцензування інфраструктурних елементів ринку з диференційованими вимогами для різних типів сервісів;
- Створити реєстр ліцензованих постачальників інфраструктурних послуг.

Ринок віртуальних активів підпорядковується закономірностям мережевої економіки [173], де цінність інфраструктури зростає експоненційно з кількістю користувачів. Це створює необхідність державної підтримки на ранніх етапах для досягнення "критичної маси" учасників. З огляду на це доречно:

- Запровадити податкові стимули для провайдерів на період до 3 років;
- Забезпечити доступ стартапів до програм підтримки бізнесу;
- Впровадити програму грантів для розробки інфраструктурних рішень.

Теорія регуляторної інфраструктури [174] наголошує на важливості створення механізмів нагляду, моніторингу та координації для належного функціонування ринку. У контексті блокчейну особливого значення набувають інструменти автоматизованого регуляторного нагляду. З огляду на це доречно:

- Розробити стандарти регуляторної звітності для учасників ринку;
- Створити автоматизовану систему моніторингу ринку віртуальних активів;
- Забезпечити технічну інфраструктуру для аналізу транзакцій щодо AML.

Згідно з теорією технологічної стандартизації [175], встановлення єдиних стандартів є критичним для забезпечення взаємодії різних елементів інфраструктури та зниження транзакційних витрат. Блокчейн-специфічним аспектом є проблема сумісності різних блокчейн-платформ. З огляду на це доречно:

- Розробити національні стандарти блокчейн-технологій, гармонізовані з міжнародними стандартами ISO/TC 307 [50];
- Сертифікація блокчейн-рішень в критичній інфраструктурі;
- Підтримати розробку технологій крос-чейн взаємодії.

Теорія "глибокого захисту" [176] передбачає багаторівневу систему безпеки, що є особливо актуальною для блокчейн-інфраструктури, де безпека є не лише технічним, але й довірчим аспектом функціонування системи. З огляду на це доречно:

- Встановити обов'язкові вимоги до безпеки для інфраструктурних елементів;

- Створити Центр кібербезпеки блокчейн-інфраструктури;
- Запровадити стрес-тестування та аудит безпеки елементів інфраструктури.

Зокрема, в Розділі 2.1 було встановлено, що забезпечення виконання зобов'язань у блокчейн-середовищі потребує не лише правових, але й технічних інфраструктурних рішень, таких як мультипідписні гаманці, механізми умовного депонування та технічні стандарти взаємодії різних блокчейн-платформ. Крім того, як показано в Розділі 2.2, ефективне доказування неможливе без відповідної технічної інфраструктури для верифікації транзакцій та аудиту смарт-контрактів.

Для України розвиток інфраструктури ринку віртуальних активів має охоплювати як приватний, так і державний сектори, створюючи синергію між інноваційними рішеннями бізнесу та надійною регуляторною базою держави.

У приватному секторі ключовими елементами інфраструктури є:

- криптобіржі;
- кастодіальні сервіси;
- провайдери гаманців;
- платіжні системи;
- інші сервіси, які забезпечують доступ до віртуальних активів.

Для стимулювання розвитку цих елементів пропонується:

1. Запровадити прозорий процес ліцензування криптобірж та інших професійних учасників ринку, який забезпечував би належний захист споживачів без створення надмірних бар'єрів для входу.
2. Стимулювати розвиток локальних біржових майданчиків через податкові пільги, спрощені процедури реєстрації та доступ до "регуляторних пісочниць".
3. Сприяти розвитку інфраструктури для інвесторів, що відповідають вимогам інвестиційних, пенсійних фондів та страхових компаній.
4. Підтримувати розвиток платіжної інфраструктури, включаючи інтеграцію з традиційними платіжними системами та розвиток платіжних шлюзів.

5. Сприяти розвитку сервісів для забезпечення ліквідності ринку, таких як маркет-мейкери та торгівельні платформи.

У державному секторі важливими елементами інфраструктури є реєстри, системи моніторингу, аналітичні інструменти та механізми взаємодії з учасниками.

Для їх розвитку пропонується:

1. Створити державний реєстр постачальників послуг, для забезпечення прозорості ринку та доступу споживачів до інформації про учасників.
2. Розробити системи моніторингу ринку для виявлення ризиків, таких як маніпулювання, шахрайські схеми або загрози для фінансової стабільності.
3. Впровадити аналітичні інструменти для аналізу блокчейн-транзакцій з метою виявлення підозрілої активності в контексті протидії відмиванню коштів.
4. Створити механізми для статистичного обліку операцій з віртуальними активами для оцінки їхнього впливу на економіку.
5. Забезпечити інтеграцію інфраструктури ринку віртуальних активів з чинними фінансовими та інформаційними системами.

Важливим аспектом розвитку інфраструктури є забезпечення кібербезпеки та стійкості систем. Для цього пропонується:

1. Розробити стандарти безпеки для учасників ринку, включаючи вимоги до захисту інформації, управління криптографічними ключами та аудиту безпеки;
2. Обміну інформацією про загрози між учасниками та державними органами;
3. Проводити тестування для оцінки стійкості інфраструктури;
4. Забезпечити підготовку фахівців з кібербезпеки блокчейн-технологій.

Важливим є також технологічний розвиток інфраструктури:

- Технологій масштабування блокчейну;
- Рішень для підвищення конфіденційності;
- Технологій взаємодії між різними блокчейн-мережами;
- Рішень для енергоефективного функціонування блокчейн-мереж.

Для стимулювання інновацій та розвитку інфраструктури необхідно забезпечити доступ до фінансування для блокчейн-стартапів через:

- Створення інвестиційних фондів, включаючи державно-приватні партнерства;
- Надання грантів для дослідження та розробки інноваційних блокчейн-рішень;
- Сприяння доступу блокчейн-стартапів до традиційних джерел фінансування;
- Розвиток нових механізмів фінансування (краудфандинг на основі токенів).

Таким чином, розвиток інфраструктури ринку віртуальних активів є комплексним завданням, яке потребує скоординованих зусиль держави, бізнесу та експертного середовища. Запропоновані заходи дозволять створити надійну та ефективну інфраструктуру, яка забезпечить широкий доступ до блокчейн-технологій, сприятиме розвитку інновацій та залученню інвестицій в Україну.

Розробка ефективного регулювання блокчейн-технологій вимагає застосування спеціалізованої методології оцінки регуляторного впливу (далі також – "ОРВ"), адаптованої до особливостей інноваційних технологій.

Традиційні підходи до ОРВ, зосереджені на статичному аналізі витрат та вигод, не відповідають динамічній природі блокчейн-інновацій. Це обумовлює необхідність розробки нової методологічної парадигми.

ОРВ для блокчейн-технологій потребує адаптації до динамічної природи інновацій. Основними елементами такої методології є:

5. Використання моделі "траєкторії розвитку" замість аналізу витрат-вигод;
6. Застосування ймовірнісного моделювання та сценарного аналізу;
7. Розширення часового горизонту аналізу для оцінки довгострокових ефектів;
8. Впровадження механізмів перегляду та адаптації регулювання.

Запропонована методологія ґрунтується на чотирьох ключових принципах:

9. Принцип технологічної контекстуальності вимагає глибокого розуміння технічних особливостей різних типів блокчейн-систем та їх впливу на

правовідносини. Це передбачає залучення технічних експертів та диференційований аналіз для різних типів блокчейн-рішень.

10. Принцип динамічної оцінки передбачає аналіз не лише безпосередніх наслідків регулювання, але і його впливу на траєкторію технологічного розвитку та інновації через застосування сценарного моделювання.
11. Принцип багатовимірності наслідків визнає, що вплив регулювання проявляється у різних сферах: економічній, правовій, соціальній, технологічній та екологічній, що вимагає комплексного міждисциплінарного підходу.
12. Принцип інклюзивності процесу передбачає залучення широкого кола стейкхолдерів до ОРВ для врахування різних перспектив.

Методологічно процес ОРВ для блокчейн-регулювання структурується у п'ять етапів:

13. Ідентифікація проблеми та цілей регулювання з визначенням контексту.
14. Визначення регуляторних альтернатив.
15. Багатовимірна оцінка наслідків кожної альтернативи.
16. Порівняльний аналіз альтернатив з урахуванням довгострокового впливу.
17. Розробка механізмів моніторингу та перегляду регулювання.

Така методологія дозволяє забезпечити науково обґрунтований підхід до розробки регуляторних рішень, враховуючи як безпосередні наслідки для учасників ринку, так і довгострокові ефекти для технологічного розвитку.

На основі аналізу аспектів блокчейн-відносин, проведеного в Розділі 2, зокрема особливостей договірних механізмів, реалізації права власності та цивільно-правового захисту, пропонується поетапний підхід до імплементації:

18. Перший етап (0-6 місяців) – Підготовчий: розробка базових підзаконних актів та створення інституційної інфраструктури.
19. Другий етап (6-18 місяців) – Впровадження базових механізмів: класифікація віртуальних активів, правовий статус смарт-контрактів, початок ліцензування.

20. Третій етап (18-36 місяців) – Комплексне регулювання: регулювання DAO, DeFi, NFT, механізми вирішення спорів.
21. Четвертий етап (понад 36 місяців) – Вдосконалення та адаптація: регулярний перегляд нормативно-правової бази та адаптація до нових форм відносин.

Цей підхід спирається на принципи регуляторної адаптивності, що забезпечить баланс між захистом прав учасників та стимулюванням інновацій.

Регуляторні пісочниці, ефективність яких підтверджена міжнародним досвідом (Розділ 3.1), дозволяють тестувати інноваційні рішення в контрольованому середовищі. Для України пропонується:

1. Створити міжвідомчу регуляторну пісочницю.
2. Встановити чіткі критерії відбору проєктів та спрощені регуляторні вимоги.
3. Забезпечити можливість обмеженого випуску токенів для тестування.
4. Впровадити механізми моніторингу та оцінки результатів.

Щодо перехідних положень, пропонується розробити підхід, який охоплює:

1. Легалізацію наявних віртуальних активів через встановлення спрощеної процедури їхньої реєстрації та класифікації відповідно до нової системи.
2. Поступове впровадження вимог для постачальників послуг, з диференційованими термінами залежно від розміру та впливу постачальника.
3. Поетапне впровадження вимог до розкриття інформації, особливо для нових форм віртуальних активів, що дозволить учасникам адаптуватися.
4. Забезпечення правової визначеності для чинних смарт-контрактів, укладених до впровадження нового регулювання, передбачивши, що зміни в законодавстві не впливають на їх дійсність та виконання.
5. Встановлення особливого режиму оподаткування на перехідний період для стимулювання легалізації операцій з віртуальними активами.

Для ефективної імплементації регуляторних пісочниць та перехідних положень необхідна активна комунікація з учасниками ринку:

- Проведення інформаційних кампаній для роз'яснення нових правил;
- Створення консультаційних центрів для надання роз'яснень;
- Розробка детальних керівництв та інформаційних матеріалів;
- Проведення зустрічей та форумів для обговорення викликів імплементації.

Таким чином, регуляторні пісочниці та перехідні положення є важливими інструментами для ефективної імплементації нового регулювання блокчейн-технологій. Вони забезпечують баланс між інноваційністю та стабільністю, сприяють плавному переходу до нових правил та мінімізують негативні наслідки змін.

Для оцінки ефективності правового регулювання блокчейн-технологій, враховуючи договірні механізми, право власності та захист прав, проаналізовані в Розділі 2, пропонується трирівнева система критеріїв:

1. Фундаментальні критерії: визначеність, захист прав, фінансова стабільність, запобігання протиправному використанню, стимулювання інновацій.
2. Функціональні критерії: прозорість вимог, пропорційність навантаження, координація між регуляторами, адаптивність, міжнародна сумісність.
3. Операційні критерії: дотримання вимог учасниками, кількість порушень прав, динаміка розвитку ринку, обсяг інвестицій, рівень довіри.

Додатково критерії групуються за економічними, правовими, технологічними, соціальними та безпековими аспектами.

Для універсальності оцінки ефективності регулювання пропонується трирівнева система критеріїв, що розвиває методологічні підходи Baldwin & Cave [156] та Coglianese [172] щодо оцінки регуляторного впливу в інноваційних галузях:

1. Фундаментальні – відображають досягнення базових цілей регулювання. Як відзначає Baldwin et al. [156], "фундаментальні критерії визначають легітимність регуляторного режиму, його відповідність очікуванням та правовим принципам". До цього рівня належать: правова визначеність [173],

захист прав споживачів [174], фінансова стабільність [175], запобігання протиправному використанню [176] та стимулювання інновацій [177].

2. Функціональні – оцінюють процесуальні та інституційні аспекти регуляторних механізмів. За визначенням Lodge & Wegrich [178], "функціональні критерії відображають здатність регуляторної системи ефективно реалізовувати свої завдання з мінімальними транзакційними витратами". До цієї категорії належать: прозорість вимог [179], пропорційність регуляторного навантаження [180], координація між регуляторами [181], адаптивність [182] та міжнародна сумісність [183].
3. Операційні критерії – вимірюють конкретні кількісні та якісні показники ефективності регулювання. Як зазначають Coglianese & Bennear [184], "операційні критерії забезпечують можливість емпіричної верифікації результатів регуляторних заходів та їх порівняння з цільовими індикаторами". Short & Toffel [185] акцентують увагу на ключових операційних показниках, які включають: рівень дотримання вимог учасниками ринку, кількість порушень прав споживачів, динаміку розвитку ринку, обсяг інвестицій та рівень довіри до технології. Ці взаємопов'язані показники в сукупності створюють основу для комплексної оцінки ефективності регуляторних режимів у сфері інноваційних фінансових технологій, включаючи блокчейн.

Пропонується створити систему моніторингу, що включає:

- Регулярний збір статистичних даних від учасників ринку
- Проведення соціологічних досліджень серед користувачів
- Аналіз судової практики та діяльності регуляторів
- Міжнародні порівняльні дослідження
- Технічний моніторинг блокчейн-мереж

Для забезпечення прозорості пропонується регулярно публікувати звіти про стан ринку, проводити публічні обговорення результатів, створити постійну робочу групу з представників регуляторів, ринку та експертів.

Методологічне значення системи критеріїв полягає у створенні основи для постійного вдосконалення регуляторних підходів на базі емпіричних даних, що дозволяє перейти від статичної до динамічної моделі регулювання.

Таким чином, комплексна система критеріїв оцінки ефективності правового регулювання блокчейн-технологій дозволить не лише визначити успішність впроваджених змін, але й забезпечити їхню адаптацію до динамічного розвитку технологій та ринку, створюючи збалансоване регуляторне середовище, яке захищає права учасників та стимулює інновації.

ВИСНОВКИ ДО РОЗДІЛУ 4

1. Проведений аналіз напрямків вдосконалення правового регулювання блокчейн-технологій в Україні дозволяє сформувати комплексне бачення необхідних змін для створення ефективної регуляторної системи, адаптованої до специфіки цих технологій. Розроблені пропозиції охоплюють концептуальні основи, матеріально-правові аспекти, інституційні механізми, процесуальні питання та практичні інструменти імплементації.

2. Аналіз концептуальних основ регулювання виявив ключове значення принципів технологічної нейтральності та балансу між інноваціями та захистом прав. Встановлено, що ефективне регулювання блокчейн-технологій має поєднувати саморегулювання, співрегулювання та державний нагляд з акцентом на адаптивність нормативної бази до швидких технологічних змін.

3. Дослідження напрямків модернізації матеріально-правового регулювання виявило необхідність чіткого визначення правового статусу віртуальних активів і смарт-контрактів, розробки спеціальних підходів до регулювання нових форм блокчейн-відносин (DAO, DeFi, NFT), адаптації інформаційного законодавства та створення ефективної системи оподаткування операцій з віртуальними активами.

4. Аналіз інституційно-правових механізмів продемонстрував доцільність оптимізації системи регуляторів через функціональний розподіл повноважень між НБУ, НКЦПФР та Мінцифри з одночасним створенням координаційного органу. Встановлено, що розвиток саморегулювання ринку через саморегулівні організації є

важливим елементом ефективної регуляторної системи, що забезпечує гнучкість та адаптивність до інновацій.

5. Дослідження механізмів захисту прав учасників блокчейн-відносин виявило необхідність розробки спеціальних підходів до захисту права власності на віртуальні активи, встановлення вимог до професійних учасників ринку та створення ефективних механізмів вирішення спорів. Визначено, що захист прав споживачів має поєднувати традиційні правові інструменти з інноваційними технологічними рішеннями.

6. Аналіз процесуальних та інфраструктурних аспектів продемонстрував важливість розробки спеціалізованих механізмів вирішення блокчейн-спорів, правил визначення юрисдикції та розвитку інфраструктури ринку віртуальних активів. Запропоновано методологію оцінки регуляторного впливу, адаптовану до особливостей блокчейн-технологій.

7. Дослідження питань імплементації та моніторингу регулювання виявило доцільність поетапного впровадження змін, використання регуляторних пісочниць як інструменту тестування інноваційних рішень та розробки багаторівневої системи критеріїв оцінки ефективності правового регулювання (фундаментальних, функціональних та операційних).

8. Важливим внеском є розробка концепцій "розосередженої відповідальності", "регуляторних інваріантів" та "вбудованого регулювання", які формують новий підхід до регулювання децентралізованих технологій. Запропонована методологія створює основу для переходу від статичної до адаптивної моделі регулювання, що враховує динамічну природу блокчейн-інновацій і забезпечує правову визначеність, захист прав учасників та стимулювання інновацій.

В И С Н О В К И

1. У дисертації здійснено комплексне теоретичне узагальнення та запропоновано нове розв'язання наукової проблеми формування цілісної концепції регулювання блокчейн-технологій. Наукова новизна полягає в тому, що це одне з перших в українській правовій науці комплексних досліджень правового регулювання інформаційних відносин у блокчейн-середовищі.

2. Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших в українській правовій науці комплексних досліджень правового регулювання інформаційних відносин, що виникають у зв'язку із застосуванням блокчейн-технології. У результаті проведеного дослідження вперше: визначено дуалістичну правову природу блокчейн-технології; систематизовано типологію об'єктів інформаційних відносин; виявлено три типи регуляторних підходів; запропоновано три сценарії міжнародної гармонізації; виявлено специфіку механізму консенсусу. Удосконалено: класифікацію договорів з віртуальними активами; систему способів забезпечення виконання зобов'язань; концепцію трансформації права власності; положення про цивільно-правову відповідальність. Набули подальшого розвитку: положення про трансформацію принципів інформаційного права; положення про адаптацію принципу автономії волі; положення про неможливість визнання смарт-контрактів суб'єктами.

3. Визначено дуалістичну правову природу блокчейн-технології як інфраструктури децентралізованого зберігання даних та системи взаємодій на основі нових механізмів довіри. Це зумовлює необхідність комплексного правового регулювання, що поєднує технологічну нейтральність з урахуванням ключових характеристик: децентралізації, криптографічного захисту, незмінності даних та можливості автоматизованого виконання умов.

4. Інформаційні відносини у сфері блокчейн-технологій характеризуються трансформацією традиційних концепцій. Блокчейн створює парадигму зберігання та обробки даних, де правдивість інформації забезпечується не авторитетом джерела, а алгоритмами та колективною верифікацією. Це призводить до трансформації принципів свободи, достовірності та захисту інформації.

5. Систематизовано типологію суб'єктів та об'єктів блокчейн-відносин. Обґрунтовано неможливість визнання смарт-контрактів суб'єктами правовідносин, натомість виділено різноманітні категорії об'єктів: смарт-контракти як програмні об'єкти, цифрові активи як інформаційні ресурси з економічною цінністю, NFT як специфічні об'єкти подвійної природи.

6. Зміст інформаційних відносин у блокчейн-середовищі являє собою складну систему юридичних та фактичних елементів. Особливістю реалізації прав та обов'язків є їх технологічна обумовленість, де можливість здійснення прав безпосередньо залежить від володіння криптографічними ключами та дотримання технічних протоколів.

7. Цивільно-правова природа блокчейн-правочинів характеризується автоматизацією через смарт-контракти та трансформацією інститутів форми правочину, умов дійсності та механізмів реституції. Запропоновано класифікацію договорів з віртуальними активами та виділено специфічні механізми забезпечення виконання зобов'язань.

8. Право власності на віртуальні активи характеризується трансформацією класичної тріади правомочностей власника. Володіння реалізується через контроль над криптографічними ключами, користування через здійснення транзакцій, а розпорядження через передачу прав.

9. Інститут цивільно-правової відповідальності у блокчейн-середовищі характеризується специфічними підставами (порушення умов смарт-контракту, неправомірне використання ключів, недотримання протоколів) та особливим розподілом ризиків через автономію учасників у прийнятті рішень.

10. Теорія функціонального підходу до регулювання віртуальних активів розвиває концепцію регулювання фінансових інструментів шляхом класифікації токенів за їх економічною функцією (utility tokens для доступу до послуг, security tokens як аналог цінних паперів, payment tokens як засіб платежу, stablecoins як стабільна криптовалюта) та встановлення диференційованого правового режиму залежно від функціонального призначення, що дозволяє уникнути регуляторного арбітражу та забезпечити адекватний захист прав учасників.

11. Міжнародний досвід демонструє формування трьох типів регуляторних підходів (відкрито-ліберального, помірковано-регульованого, жорстко-рестриктивного), найефективнішим з яких є перший. Міжнародні організації (FATF, ISO, WIPO, G20) відіграють ключову роль у формуванні глобальних стандартів.

12. Механізми захисту прав учасників формують систему, що поєднує правові інструменти з технологічними рішеннями. Регулювання нових форм блокчейн-відносин (DeFi, DAO, NFT) знаходиться на початковому етапі та потребує інноваційних регуляторних рішень.

13. Перспективи міжнародної гармонізації регулювання блокчейн-технологій пов'язані з формуванням глобальної регуляторної екосистеми. Найбільш імовірним є сценарій регіональної гармонізації з формуванням регуляторних блоків, що відповідає загальним тенденціям розвитку глобального фінансового регулювання.

14. Концептуальні основи вдосконалення регулювання в Україні мають ґрунтуватися на принципах технологічної нейтральності та балансу між інноваціями та захистом прав. Модернізація потребує комплексного підходу: визначення правового статусу віртуальних активів і смарт-контрактів, регулювання нових форм відносин, розробки системи оподаткування.

15. Інституційно-правові механізми мають забезпечувати функціональний розподіл повноважень між НБУ, НКЦПФР та Мінцифри. Механізми захисту прав учасників потребують адаптації до специфіки технологій, включаючи створення цифрового депозитарію, впровадження процедур вирішення спорів та механізмів компенсації.

16. Процесуальні аспекти вимагають розробки спеціалізованих механізмів вирішення блокчейн-спорів, правил юрисдикції та розвитку інфраструктури ринку. Імплементація потребує поетапного підходу (підготовчий, впровадження, комплексне регулювання, адаптація) з використанням регуляторних пісочниць.

17. В основу авторської концепції регулювання блокчейн-технологій покладено положення, що розвивають чинні доктрини: концепція "розосередженої відповідальності", теорія "регуляторних інваріантів" та парадигма "вбудованого

регулювання". Це формує фундамент для нової парадигми регулювання децентралізованих систем.

18. Запропонована концепція враховує технологічні особливості, специфіку інформаційних відносин та міжнародний досвід, спрямована на створення збалансованої системи, що забезпечує правову визначеність, захист прав та стимулювання інновацій у цифровій економіці України.

С П И С О К В И К О Р И С Т А Н И Х Д Ж Е Р Е Л

1. Legal Aspects of Blockchain / J. Naves et al. Innovations: Technology, Governance, Globalization. 2019. Vol. 12, no. 3–4. P. 88–93. URL: https://doi.org/10.1162/inov_a_00278 (дата звернення: 29.08.2023).

2. De Filippi P., Mannan M., Reijers W. Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society. 2020. Vol. 62. P. 101284. URL: https://doi.org/10.1016/j.techsoc.2020.101284 (дата звернення: 29.08.2023).

3. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press. URL: https://doi.org/10.1515/9781400884254 (дата звернення: 28.08.2023).

4. Кравченко П. М., Скрябін Б. О., Дубініна О. М., Курбатов С. В. Блокчейн і децентралізовані системи : навч. посібник у 3 ч. Ч. 1. Харків : Видавництво "ТОЧКА", 2019. 452 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/41855 (дата звернення: 28.08.2023).

5. Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. Information & Communications Technology Law, 26(2), 116-134. URL: https://doi.org/10.1080/13600834.2017.1301036 (дата звернення: 01.09.2023).

6. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 12.08.2023).

7. Цивільний кодекс України : Кодекс України від 16.01.2003 р. № 435-IV : станом на 10 черв. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 28.08.2023).

8. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 15.09.2023).

9. Борисова А. "Інформація" та "правова інформація" як об'єкти правовідносин у сфері інформаційних комунікацій. Юридичний вісник. 2020. № 4. С. 180–188. URL: https://doi.org/10.32837/yuv.v0i4.1987 (дата звернення: 02.10.2023).

10. Bashir I. Blockchain Consensus. Blockchain Consensus. Berkeley, CA, 2022. P. 207–257. URL: https://doi.org/10.1007/978-1-4842-8179-6_5 (дата звернення: 28.08.2023).

11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260. URL: https://bitcoin.org/bitcoin.pdf (дата звернення: 28.08.2023).

12. A Blockchain-based Educational Digital Assets Management System / J. Li et al. IFAC-PapersOnLine. 2020. Vol. 53, no. 5. P. 47–52. URL: https://doi.org/10.1016/j.ifacol.2021.04.082 (дата звернення: 28.08.2023).

13. Інформаційне право України : навчальний посібник / А. М. Куліш, Т. А. Кобзєва, В. С. Шапіро. – Суми : Сумський державний університет, 2016. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/45286/1/Kulish.pdf (дата звернення: 21.09.2023).

14. Deloitte. 2021 Global Blockchain Survey. Deloitte Insights. 2021. URL: https://www2.deloitte.com/content/dam/insights/articles/US144337_Blockchain-survey/DI_Blockchain-survey.pdf (дата звернення: 15.03.2024).

15. Kushwaha, S.S., Joshi, S., Singh, D., Kaur, M., & Lee, H.-N. (2022). Ethereum Smart Contract Analysis Tools: A Systematic Review. IEEE Access, 10, 57037-57062. DOI: 10.1109/ACCESS.2022.3169902. URL: https://ieeexplore.ieee.org/document/9762279 (дата звернення: 10.11.2023).

16. Finck M. Blockchain Governance. Blockchain Regulation and Governance in Europe. Cambridge University Press. 2018. URL: https://doi.org/10.1017/9781108609708.007 (дата звернення: 12.05.2024).

17. SEC v. Telegram Group Inc., 448 F. Supp. 3d 352. Casetext. США. 2020. URL: https://casetext.com/case/sec-exch-commn-v-telegram-grp-inc (дата звернення: 10.07.2024).

18. Schär F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review. 2021. Vol. 103 (2). URL: https://doi.org/10.20955/r.103.153-174 (дата звернення: 24.05.2024).

19. Berryhil J., Bourgery T., Hanson A. Blockchains Unchained Blockchain Technology and its Use in the Public Sector. OECD Working Papers on Public Governance No. 28. 2018. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2018/06/blockchains-unchained_fcbd568f/3c32c429-en.pdf (дата звернення: 03.02.2025).

20. Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416-3452. URL: https://doi.org/10.1109/COMST.2018.2842460 (дата звернення: 12.10.2023).

21. Key Features. Handbook of Research on Blockchain Technology. 2020. P. xxxi. URL: https://doi.org/10.1016/b978-0-12-819816-2.00024-1 (дата звернення: 15.01.2024).

22. Chang V. et al. How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. Technological Forecasting and Social Change. 2020. Vol. 158. P. 120166. URL: https://doi.org/10.1016/j.techfore.2020.120166 (дата звернення: 25.10.2023).

23. Pazaitis A., De Filippi P., Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. Technological Forecasting and Social Change. 2017. Vol. 125. P. 105–115. URL: https://doi.org/10.1016/j.techfore.2017.05.025 (дата звернення: 11.11.2024).

24. When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry / A. Bayle et al. 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, 3–6 December 2018. URL: https://doi.org/10.1109/wi.2018.00133 (дата звернення: 01.09.2023).

25. Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. Artificial Intelligence and Law, 26(4), 377-409. URL: https://doi.org/10.1007/s10506-018-9223-3 (дата звернення: 27.04.2024).

26. Politou, E., Alepis, E., & Patsakis, C. (2019). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. Journal of Cybersecurity, 4(1), tyy001. URL: https://doi.org/10.1093/cybsec/tyy001 (дата звернення: 16.11.2024).

27. Singh, A., Parizi, R.M., Zhang, Q., Choo, K.-K.R., & Dehghantanha, A. (2020). Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security, 88, 101654. DOI: 10.1016/j.cose.2019.101654. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404818310927 (дата звернення: 24.04.2024).

28. Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). Shaping the future of Ethereum: exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. Frontiers in Blockchain, 4, 1151724. URL: https://doi.org/10.3389/fbloc.2023.1151724 (дата звернення: 25.10.2023).

29. Wang, X., Yi, P., & Zhou, L. (2024). Opportunity or opportunism? Blockchain technology adoption and corporate default risk. Humanities and Social Sciences Communications, 11, 1360. DOI: 10.1038/s41599-024-03727-6. URL: https://www.nature.com/articles/s41599-024-03727-6 (дата звернення: 25.10.2023).

30. Wu, H., Yao, Q., Liu, Z., Huang, B., Zhuang, Y., Tang, H., & Liu, E. (2024). Blockchain for finance: A survey. IET Blockchain, 1(1), 5-21. DOI: 10.1049/blc2.12067. URL: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/blc2.12067 (дата звернення: 15.09.2023).

31. Ethereum Foundation. The Merge: How Ethereum's Carbon Footprint Is About To Drop by Over 99%. 2022. URL: https://ethereum.org/en/energy-consumption/ (дата звернення: 05.04.2024).

32. Dutta P., Choi T.-M. et al. Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation Research Part E: Logistics and Transportation Review. 2020. Vol. 142. P. 102067. URL: https://doi.org/10.1016/j.tre.2020.102067 (дата звернення: 12.10.2023).

33. Blockchain Council. Ethereum 2.0: A Complete Guide on The Merge. 2023. URL: https://www.blockchain-council.org/ethereum/ethereum-2-0/ (дата звернення: 15.03.2024).

34. Kamble, S., Gunasekaran, A., & Arha, H. (2019). Understanding the blockchain technology adoption in supply chains-Indian context. International Journal of Production

Research, 57(7), 2009-2033. URL: https://doi.org/10.1080/00207543.2018.1518610 (дата звернення: 12.10.2023).

35. Lahlou I., Motaki N. Integrating Blockchain with ERP systems for better supply chain performance. 2022 14th International Colloquium of Logistics and Supply Chain Management (LOGISTIQUA), El Jadida, Morocco, 25–27 May 2022. URL: https://doi.org/10.1109/logistiqua55056.2022.9938086 (дата звернення: 12.10.2023).

36. Hu K., Li Y., Li Z. et al. Smart Contract Engineering. Electronics. 2020. Vol. 9, no. 12. P. 2042. URL: https://doi.org/10.3390/electronics9122042 (дата звернення: 10.03.2024).

37. Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective / J. Ellul et al. ERA Forum. 2020. Vol. 21, no. 2. P. 209–220. URL: https://doi.org/10.1007/s12027-020-00617-7 (дата звернення: 02.10.2023).

38. CNIL. Blockchain et RGPD: Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles. 2018. URL: https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles (дата звернення: 16.11.2024).

39. Xu X., Weber I., Staples M. Architecture for Blockchain Applications. Springer International Publishing, 2019. URL: https://doi.org/10.1007/978-3-030-03035-3 (дата звернення: 22.11.2024).

40. Subramanian H. et al. Blockchain Regulations and Decentralized Applications. Communications of the Association for Information Systems. 2020. Vol. 47, no. 1. P. 189–207. URL: https://doi.org/10.17705/1cais.04709 (дата звернення: 15.01.2024).

41. SEC v. Ripple Labs Inc., No. 20-cv-10832 (S.D.N.Y. July 13, 2023). URL: https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf (дата звернення: 11.11.2024).

42. In re Celsius Network LLC, 23-33518 (Bankr. S.D.N.Y. Jan. 4, 2023). URL: https://cases.stretto.com/celsius/court-docket/key-documents/ (дата звернення: 28.11.2024).

43. In re FTX Trading Ltd., No. 22-11068 (Bankr. D. Del. filed Nov. 11, 2022). URL: https://cases.ra.kroll.com/FTX/Home-DocketInfo (дата звернення: 28.11.2024).

44. Hafid A., Hafid A. S., Samih M. Scaling Blockchains: A Comprehensive Survey. IEEE Access. 2020. Vol. 8. P. 125244-125262. URL: https://doi.org/10.1109/ACCESS.2020.3007251 (дата звернення: 29.11.2024).

45. Belchior R., Vasconcelos A., Guerreiro S., Correia M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Computing Surveys. 2021. URL: https://doi.org/10.1145/3471140 (дата звернення: 29.11.2024).

46. Mehar M. I. et al. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. Journal of Cases on Information Technology. 2019. Vol. 21, no. 1. P. 19-32. URL: https://doi.org/10.4018/JCIT.2019010102 (дата звернення: 29.11.2024).

47. Fernando F. et al. Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1). FinTech Notes. 2021. T. 2021, № 002. URL: https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654 (дата звернення: 12.06.2024).

48. Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2019). The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators. Harvard International Law Journal, 60(2), 267-315. URL: https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/3_ICO_60.2.pdf (дата звернення: 27.11.2024).

49. Nicolle E. FTX Sues Binance, Ex-CEO Zhao Seeking $1.8 Billion Clawback. Bloomberg. 2024. URL: https://www.bloomberg.com/news/articles/2024-11-11/ftx-sues-binance-former-ceo-zhao-seeking-1-8-billion-clawback (дата звернення: 11.11.2024).

50. ISO. Blockchain and distributed ledger technologies — Overview of ISO/TC 307 standardization work. 2022. URL: https://www.iso.org/committee/6266604.html (дата звернення: 16.11.2024).

51. Fisch C. Initial coin offerings (ICOs) to finance new ventures. University of Luxembourg - Interdisciplinary Centre for Security, Reliability and Trust (SnT). 2018. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3147521 (дата звернення: 27.11.2024).

52. Bank for International Settlements. Central bank digital currencies: foundational principles and core features. Basel, 2020. URL: https://www.bis.org/publ/othp33.pdf (дата звернення: 12.05.2024).

53. Chainalysis. The 2023 Crypto Crime Report. 2024. URL: https://go.chainalysis.com/2023-crypto-crime-report.html (дата звернення: 15.12.2024).

54. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13, e00151. DOI: 10.1016/j.jbvi.2019.e00151. URL: https://www.sciencedirect.com/science/article/abs/pii/S2352673419300824 (дата звернення: 12.05.2024).

55. Ali, O., Ally, M., & Dwivedi, Y. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management, 54, 102199. DOI: 10.1016/j.ijinfomgt.2020.102199. URL: https://www.sciencedirect.com/science/article/abs/pii/S0268401219310928 (дата звернення: 25.10.2023).

56. Zheng Wei C. C., Wen C. C. Blockchain-Based Electronic Voting Protocol. JOIV : International Journal on Informatics Visualization. 2018. Т. 2, № 4-2. С. 336. URL: https://doi.org/10.30630/joiv.2.4-2.174 (дата звернення: 29.09.2023).

57. Jafar, U., Ab Aziz, M.J., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors, 21(17), 5874. DOI: 10.3390/s21175874. URL: https://www.mdpi.com/1424-8220/21/17/5874 (дата звернення: 10.11.2023).

58. Negara E. S. et al. A Survey Blockchain and Smart Contract Technology in Government Agencies. IOP Conference Series: Materials Science and Engineering. 2021. Vol. 1071. URL: https://doi.org/10.1088/1757-899x/1071/1/012026 (дата звернення: 10.11.2023).

59. Antonopoulos A. M. Mastering Bitcoin: Programming the Open Blockchain. 2nd Edition. O'Reilly Media, 2017. URL: https://github.com/bitcoinbook/bitcoinbook (дата звернення: 15.01.2024).

60. Van Hijfte S. ICO. Blockchain and Regulation. Berkeley, CA, 2021. URL: https://doi.org/10.1007/978-1-4842-7968-7_3 (дата звернення: 10.12.2023).

61. Bertolini A., Episcopo F. Robots and AI as Legal Subjects? Disentangling the Ontological and Functional Perspective. Frontiers in Robotics and AI. 2022. Vol. 9. URL: https://doi.org/10.3389/frobt.2022.842213 (дата звернення: 15.01.2024).

62. Vilalta Nicuesa A. E. Smart Legal Contracts. International Journal of Online Dispute Resolution. 2019. Vol. 6, no. 2. P. 239–242. URL: https://doi.org/10.5553/ijodr/235250022019006002017 (дата звернення: 15.01.2024).

63. Aznar E. Legal challenges and structures of Decentralised Autonomous Organisations (DAOs): A brief analysis for the current legal framework. LegalCripto by BAES. 2024. URL: https://www.baeslegalcripto.eu/legalcripto/en/legal-challenges-and-structures-of-daos/ (дата звернення: 22.01.2025).

64. Kleros. A fully decentralized arbitration system. Kleros.io. 2023. URL: https://kleros.io/ (дата звернення: 11.11.2024).

65. Schulz K. A., Gstrein O. J., Zwitter A. J. Exploring the governance and implementation of sustainable development initiatives through blockchain technology. Futures. 2020. Vol. 122. P. 102611. URL: https://doi.org/10.1016/j.futures.2020.102611 (дата звернення: 15.01.2024).

66. Curley N. Blockchain Disruption: Digital Assets Are Changing How We Do Business. SMU Science and Technology Law Review. 2022. Vol. 25, no. 2. P. 265. URL: https://doi.org/10.25172/smustlr.25.2.6 (дата звернення: 02.03.2024).

67. Custers B., Overwater L. Regulating Initial Coin Offerings and Cryptocurrencies: A Comparison of Different Approaches in Nine Jurisdictions Worldwide. European Journal of Law and Technology, Vol. 10, Issue 3, 2019. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3527469 (дата звернення: 27.11.2024).

68. 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, L 150, 2023, p. 1–43. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02023R1114-20240109 (дата звернення: 11.11.2024).

69. Ministry of Economy, Trade and Industry (METI), Japan. The WEB3 white paper. 2024. URL: https://www.taira-m.jp/The%20web3%20White%20Paper%202024%EF%BC%88English%2Cver%29.pdf (дата звернення: 11.11.2024).

70. CoinGecko. Digital Assets Market Report Q1 2024. 2024. URL: https://www.coingecko.com/research/publications/2024-q1-crypto-report (дата звернення: 15.04.2024).

71. Baker B., Pizzo A., Su Y. Non-Fungible Tokens. Sports Innovation Journal. 2022. Vol. 3. P. 1–15. URL: https://doi.org/10.18060/25636 (дата звернення: 03.03.2024).

72. Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447. URL: https://doi.org/10.48550/arXiv.2105.07447 (дата звернення: 03.03.2024).

73. Yeom H. Legal Issues of Intellectual Property Rights in NFT. The Justice. 2023. Vol. 194. P. 85–125. URL: https://doi.org/10.29305/tj.2023.2.194.85 (дата звернення: 03.03.2024).

74. Sestino A., Guido G., Peluso A. M. Non-Fungible Tokens (NFTs). Cham : Springer International Publishing, 2022. URL: https://doi.org/10.1007/978-3-031-07203-1 (дата звернення: 03.03.2024).

75. Hammi B., Zeadally S., Perez A. J. Non-Fungible Tokens: A Review. IEEE Internet of Things Magazine. 2023. Vol. 6, no. 1. P. 46–50. URL: https://doi.org/10.1109/iotm.001.2200244 (дата звернення: 03.03.2024).

76. Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. IEEE Access, 10, 70746-70759. DOI: 10.1109/ACCESS.2022.3187688. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9812616 (дата звернення: 03.03.2024).

77. Taş R., Tanrıöver Ö. Ö. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. Symmetry. 2020. Vol. 12, no. 8. P. 1328. URL: https://doi.org/10.3390/sym12081328 (дата звернення: 10.03.2024).

78. Грохольський В. Л. Актуальні питання правового регулювання інформаційних відносин в Україні. South Ukrainian Law Journal. 2020. № 3. С. 141–145. URL: https://doi.org/10.32850/sulj.2020.3.25 (дата звернення: 15.09.2023).

79. Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: foundations, design landscape and research directions. arXiv preprint arXiv:1608.00771. URL: https://doi.org/10.48550/arXiv.1608.00771 (дата звернення: 29.09.2023).

80. Diega G. N. Blockchains, smart contracts, and copyright law. Proceedings of the Institute of State and Law of the RAS. 2019. T. 14, № 3. URL: https://doi.org/10.35427/2073-4522-2019-14-3-notoladiega (дата звернення: 27.04.2024).

81. Mik, E. (2017). Smart contracts: terminology, technical limitations and real world complexity. Law, Innovation and Technology, 9(2), 269-300. URL: https://doi.org/10.1080/17579961.2017.1378468 (дата звернення: 12.05.2024).

82. Vigliotti, M.G. (2021). What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts. Frontiers in Blockchain, 3. DOI: 10.3389/fbloc.2020.553671. URL: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.553671/full (дата звернення: 12.06.2024).

83. UK Jurisdiction Taskforce. Legal Statement on Cryptoassets and Smart Contracts. 2019. URL: https://www.judiciary.uk/wp-content/uploads/2020/02/UKJT-Statement-on-cryptoassets-and-smart-contracts-1.pdf (дата звернення: 10.07.2024).

84. Estcourt J. S. Smart Contracts and Dispute Resolution. Smart Legal Contracts. 2022. P. 79–87. URL: https://doi.org/10.1093/oso/9780192858467.003.0005 (дата звернення: 10.03.2024).

85. Lauslahti, K., Mattila, J., & Seppälä, T. (2017). Smart contracts–how will blockchain technology affect contractual practices? The Research Institute of the Finnish Economy (ETLA) Brief, 68. URL: https://www.etla.fi/wp-content/uploads/ETLA-Brief-68.pdf (дата звернення: 10.03.2024).

86. Ouyang L., Zhang W., Wang F.-Y. Intelligent contracts: Making smart contracts smart for blockchain intelligence. Computers and Electrical Engineering. 2022. Vol. 104. P. 108421. URL: https://doi.org/10.1016/j.compeleceng.2022.108421 (дата звернення: 27.04.2024).

87. De Filippi, Primavera, and Aaron Wright. Blockchain and the Law: The Rule of Code. Harvard University Press, 2018. URL: https://doi.org/10.2307/j.ctv2867sp.4 (дата звернення: 12.05.2024).

88. Стази А. Smart Contracts: Legal Issues and First Regulatory Approaches. Smart Contracts and Comparative Law. Cham, 2021. P. 71–106. URL: https://doi.org/10.1007/978-3-030-83240-7_4 (дата звернення: 02.03.2024).

89. P. Digital Privacy, Personal Data Protection and the Legal Framework for Blockchain Technology. Frontiers in Blockchain. 2022. Vol. 5. URL: https://doi.org/10.3389/fbloc.2022.776836 (дата звернення: 15.08.2024).

90. Szabo N. Formalizing and Securing Relationships on Public Networks. First Monday. 1997. Vol. 2, no. 9. URL: https://doi.org/10.5210/fm.v2i9.548 (дата звернення: 24.04.2024).

91. Vigliotti M. G. What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts. Frontiers in Blockchain. 2021. Vol. 3. URL: https://doi.org/10.3389/fbloc.2020.553671 (дата звернення: 15.01.2024).

92. Redden J. Global Internet Value and Work. Perspectives on Global Development and Technology. 2018. Vol. 17, no. 3. P. 341–350. URL: https://doi.org/10.1163/15691497-12341482 (дата звернення: 10.03.2024).

93. Liu, Y., & Tsyvinski, A. (2021). Risks and returns of cryptocurrency. The Review of Financial Studies, 34(6), 2689-2727. URL: https://doi.org/10.1093/rfs/hhaa113 (дата звернення: 02.03.2024).

94. Casi-Casanova, A., & García-Benau, M. A. (2021). Tax regulation on blockchain and cryptocurrency: The implications for open innovation. Journal of Innovation Economics & Management, 1(34), 237-263. URL: https://doi.org/10.3917/jie.pr1.0137 (дата звернення: 27.04.2024).

95. Wang, R. (2024). Unwinding NFTs in the shadow of IP law. American Business Law Journal, 61(2), 245-290. DOI: 10.1111/ablj.12237. URL: https://onlinelibrary.wiley.com/doi/full/10.1111/ablj.12237 (дата звернення: 27.04.2024).

96. Hashemi M. To coordinate or not to coordinate: The governance of digital assets in a global marketplace. Ohio Northern University International Law Journal. Volume 2.

2024. URL: https://digitalcommons.onu.edu/cgi/viewcontent.cgi?params=/context/ilj/article/1018/&path_info=To_Coordinate_or_Not_to_Coordinate__The_Governance_of_Digital_Assets_in_a_Global_Marketplace.pdf (дата звернення: 22.01.2025).

97. De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code. Harvard University Press. URL: https://doi.org/10.2307/j.ctv2867sp (дата звернення: 05.04.2024).

98. European Central Bank. Virtual currency schemes – a further analysis. Frankfurt am Main, 2015. С. 11–13. URL: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (дата звернення: 12.05.2024).

99. FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Financial Action Task Force, 2021. URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html (дата звернення: 16.11.2024).

100. World Economic Forum. Decentralized Autonomous Organization Toolkit. 2023. URL: https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organization_Toolkit_2023.pdf (дата звернення: 10.02.2025).

101. Financial Action Task Force (FATF). Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. 2020. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf (дата звернення: 05.05.2024).

102. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX : станом на 15 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2074-20 (дата звернення: 12.06.2024).

103. Global Legal Research Directorate Staff. Regulation of Cryptocurrency Around the World. The Law Library of Congress, 2021. URL: https://www.loc.gov/law/help/cryptocurrency/world-survey.php (дата звернення: 24.05.2024).

104. Kraizberg, E. (2023). Non-fungible tokens: a bubble or the end of an era of intellectual property rights. Financial Innovation, 9, 32. DOI: 10.1186/s40854-022-00428-4. URL: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-022-00428-4 (дата звернення: 18.07.2024).

105. United States Patent and Trademark Office, United States Copyright Office. (2024). Non-Fungible Tokens and Intellectual Property: A Report to Congress. March 12, 2024. URL: https://www.uspto.gov/ip-policy/joint-study-intellectual-property-rights-and-non-fungible-tokens (дата звернення: 18.07.2024).

106. Tiwari M., Gangmei G., Kumar Y. Issues with Private Key Management in Blockchain Wallets. International Journal of Advanced Research in Computer Science. 2021. Vol. 12, no. 3. P. 19-24. URL: https://doi.org/10.26483/ijarcs.v12i3.6752 (дата звернення: 20.01.2025).

107. Kamath R. Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. The Journal of The British Blockchain Association. 2018. Vol. 1, no. 1. URL: https://doi.org/10.31585/jbba-1-1-(10)2018 (дата звернення: 11.12.2024).

108. Baur D. G., Hong K., Lee A. Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions & Money. 2018. № 54. URL: https://doi.org/10.1016/j.intfin.2017.12.004 (дата звернення: 24.05.2024).

109. Fairfield, J. (2021). Tokenized: The law of non-fungible tokens and unique digital property. Indiana Law Journal, 97(4), 1261-1313. URL: https://www.repository.law.indiana.edu/ilj/vol97/iss4/4/ (дата звернення: 10.07.2024).

110. Про валюту і валютні операції : Закон України від 21.06.2018 р. № 2473-VIII : станом на 1 квіт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2473-19 (дата звернення: 12.06.2024).

111. Dirwono W. Blockchain and Intellectual Property Protection: Current Applications and Future Trends. International Journal of Intellectual Property Management. 2023. Vol. 13, no. 2. P. 135-152. URL: https://doi.org/10.1504/IJIPM.2023.132025 (дата звернення: 05.09.2024).

112. Liechtenstein Blockchain Act (Token and Trustworthy Technology Service Providers Act). Government of the Principality of Liechtenstein. 2019. URL:

https://www.ecri.eu/system/tdf/thomas_duenser_1.pdf?file=1=node=1%2055=0 (дата звернення: 11.11.2024).

113. Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. Journal of Financial Regulation, 6(2), 172-203. URL: https://doi.org/10.1093/jfr/fjaa010 (дата звернення: 12.06.2024).

114. Finck, M., & Moscon, V. (2019). Copyright law on blockchains: Between new forms of rights administration and digital rights management 2.0. IIC - International Review of Intellectual Property and Competition Law, 50(1), 77-108. URL: https://doi.org/10.1007/s40319-018-00776-8 (дата звернення: 21.11.2024).

115. Bitfury & Government of Georgia. Blockchain for Land Titling. White Paper, 2016. URL: https://bitfury.com/content/downloads/the_bitfury_group_republic_of_georgia_expand_blockchain_pilot_2_7_16.pdf (дата звернення: 22.01.2025).

116. Бернська конвенція про охорону літературних і художніх творів : Конвенція Всесвіт. орг. інтелект. власності від 24.07.1971 : станом на 31 трав. 1995 р. URL: https://zakon.rada.gov.ua/laws/show/995_051 (дата звернення: 10.07.2024).

117. Nam J., Lee S., Park S., Lee I. IP dLedger - Decentralized ledger for intellectual property administration. Technological Forecasting and Social Change. Volume 186, Part A. 2023. URL: https://www.sciencedirect.com/science/article/pii/S0040162522006266 (дата звернення: 15.08.2024).

118. Estato M., Frediani A. Crafting the Future of Finance: A Comparative Analysis of Cryptocurrency Regulation in the Global Economy. Centre for Commercial Law Studies, Queen Mary University of London, London, UK. Vol.13 No.1. 2024. URL: https://www.scirp.org/journal/paperinformation?paperid=132187 (дата звернення: 22.01.2025).

119. Singapore PDPC (Personal Data Protection Commission). Blockchain Guide final. 2023. URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Blockchain-Guide_final.pdf (дата звернення: 21.11.2024).

120. European Union Blockchain Observatory & Forum. Blockchain and Intellectual Property. 2020. URL: https://blockchain-

observatory.ec.europa.eu/document/download/2df0bb3c-61fd-4ac6-921b-ff50fc32aeb9_en?filename=report_conclusion_book_v1.0.pdf&prefLang=es (дата звернення: 21.11.2024).

121. Xu R., Zhang L., Zhao H., Peng Y. Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology. 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS). 2017. P. 128-133. URL: https://doi.org/10.1109/ISADS.2017.21 (дата звернення: 12.02.2025).

122. Allen, D.W.E., Berg, C., Davidson, S. et al. International Policy Coordination for Blockchain Supply Chains. Asia & the Pacific Policy Studies. 2020. Vol. 7, no. 3. P. 394-407. URL: https://doi.org/10.1002/app5.281 (дата звернення: 12.02.2025).

123. Mik E. Smart Contracts: Illusions and Expectations. Journal of Strategic Contracting and Negotiation. 2020. Vol. 5. No. 1-2. P. 3-20. URL: https://doi.org/10.1177/2055563620954927 (дата звернення: 12.02.2025).

124. UAE Government Portal. Emirates Blockchain Strategy 2021. 2018. URL: https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021 (дата звернення: 03.02.2025).

125. AA v. Persons Unknown & Ors, Re Bitcoin [2019] EWHC 3556 (Comm). England and Wales High Court (Commercial Court). 2019. URL: https://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html (дата звернення: 05.01.2025).

126. International Organization of Securities Commissions (IOSCO). DeFi Market Trends, Risks and Regulation. 2022. URL: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf (дата звернення: 10.06.2024).

127. Hermès International v. Mason Rothschild, No. 22-cv-384 (S.D.N.Y. Feb. 8, 2023). URL: https://www.nysd.uscourts.gov/sites/default/files/2023-02/22cv0384-2023-02-08.pdf (дата звернення: 12.02.2025).

128. European Commission. DLT Pilot Regime: Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology. 2022. URL: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/financial-

markets/regulatory-frameworks-financial-markets/markets-financial-instruments-directive-mifid/distributed-ledger-technology-pilot-regime_en (дата звернення: 10.05.2024).

129. Federal Trade Commission. FTC Investigates into Coinbase's Operations. 2023. URL: https://www.ftc.gov/legal-library/browse/crypto-related-investigations (дата звернення: 25.05.2024).

130. Hacker P., Lianos I. Regulating Blockchain: Techno-social and Legal Challenges. Oxford University Press. 2022. URL: https://doi.org/10.1093/oso/9780198842187.001.0001 (дата звернення: 03.03.2025).

131. Marks G., Hooghe L. Multi-level Governance and European Integration. Rowman & Littlefield, 2021. URL: https://doi.org/10.2307/j.ctvb1htc4 (дата звернення: 15.01.2025).

132. PwC Switzerland. Crypto Valley Report 2022: Swiss Blockchain Ecosystem Analysis. 2022. URL: https://www.pwc.ch/en/publications/2022/crypto-valley-report-2022.pdf (дата звернення: 10.03.2024).

133. Swiss Financial Market Supervisory Authority (FINMA). Annual Report on Crypto Compliance. 2023. URL: https://www.finma.ch/en/documentation/finma-publications/reports/annual-reports/ (дата звернення: 22.01.2025).

134. Hacker P., Dimitropoulos G. Blockchain Governance and Regulation in Global Perspective. Oxford University Press. 2022. URL: https://doi.org/10.1093/oso/9780197639566.001.0001 (дата звернення: 12.01.2025).

135. Zetzsche D., Arner D., Buckley R. Decentralized Finance (DeFi): Policy and Regulatory Challenges of a Global Financial Transformation. Journal of Financial Regulation. 2023. Vol. 9, no. 1. P. 47-75. URL: https://doi.org/10.1093/jfr/fjac012 (дата звернення: 20.12.2024).

136. WIPO. WIPO Blockchain White Paper: Integrating DLT in Intellectual Property Ecosystems. World Intellectual Property Organization, 2021. URL: https://www.wipo.int/export/sites/www/cws/en/pdf/blockchain-for-ip-ecosystem-whitepaper.pdf (дата звернення: 16.11.2024).

137. WTO. Blockchain and DLT in Trade: A REALITY CHECK. World Trade Organization, 2019. URL:

https://www.wto.org/english/res_e/booksp_e/blockchainrev19_e.pdf (дата звернення: 16.11.2024).

138. UNCITRAL. Taxonomy of legal issues related to the digital economy. 2023. URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/digitaleconomytaxonomy.pdf (дата звернення: 16.11.2024).

139. 139. European Commission. Proposal for a Council Directive amending Directive 2011/16/EU on administrative cooperation in the field of taxation (DAC8). 2022. URL: https://www.bfn.se/wp-content/uploads/remiss-av-dac-8-forslag-fran-komcleaned.pdf (дата звернення: 11.12.2024).

140. Tiwari, M., Gepp, A., & Kumar, K. (2020). The future of raising finance: a new opportunity to commit fraud? A review of initial coin offering (ICOs) frauds. Crime, Law and Social Change, 73(2), 249-288. URL: https://doi.org/10.1007/s10611-019-09873-2 (дата звернення: 11.12.2024).

141. Про фінансові послуги та державне регулювання ринків фінансових послуг : Закон України від 12.07.2001 р. № 2664-III : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2664-14 (дата звернення: 15.03.2025).

142. Про товариства з обмеженою та додатковою відповідальністю : Закон України від 06.02.2018 р. № 2275-VIII : станом на 15 трав. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2275-19 (дата звернення: 12.05.2024).

143. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII : станом на 10 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3792-12 (дата звернення: 25.01.2024).

144. Податковий кодекс України : Кодекс від 02.12.2010 р. № 2755-VI : станом на 1 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2755-17 (дата звернення: 05.04.2024).

145. Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-XII : станом на 1 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3687-12 (дата звернення: 05.04.2024).

146. Про охорону прав на знаки для товарів і послуг : Закон України від 15.12.1993 р. № 3689-XII : станом на 1 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/3689-12 (дата звернення: 05.04.2024).

147. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 15.01.2024).

148. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII : станом на 1 бер. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 05.03.2024).

149. Lessig L. Code and Other Laws of Cyberspace. Basic Books, 1999. URL: https://doi.org/10.1002/asi.1103120414 (дата звернення: 10.04.2024).

150. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.01.2024).

151. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI : станом на 1 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 10.04.2024).

152. Про електронну комерцію : Закон України від 03.09.2015 р. № 675-VIII : станом на 1 лют. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/675-19 (дата звернення: 15.02.2024).

153. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 15.01.2024).

154. Japan Digital Asset Exchange Association (JDXA). Self-Regulatory Rules for Virtual Asset Exchanges. 2022. URL: https://jdxa.or.jp/en/regulatory-framework/self-regulatory-rules/ (дата звернення: 15.01.2025).

155. Williamson O. E. The New Institutional Economics: Taking Stock, Looking Ahead. Journal of Economic Literature. 2000. Vol. 38, No. 3. P. 595-613. URL: https://doi.org/10.1257/jel.38.3.595 (дата звернення: 20.11.2024).

156. Baldwin R., Cave M., Lodge M. Understanding Regulation: Theory, Strategy and Practice. 2nd ed. Oxford University Press, 2012. URL: https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001 (дата звернення: 15.12.2024).

157. Quintyn M., Taylor M. Regulatory and Supervisory Independence and Financial Stability. IMF Working Paper WP/07/126. 2007. URL: https://www.imf.org/external/pubs/ft/wp/2007/wp07126.pdf (дата звернення: 10.10.2024).

158. Lavrijssen S., Ottow A. Independent Supervisory Authorities: A Fragile Concept. Legal Issues of Economic Integration. 2014. Vol. 41, No. 4. P. 419-446. URL: https://doi.org/10.54648/leie2014028 (дата звернення: 07.12.2024).

159. Black J. Regulatory Conversations. Journal of Law and Society. 2013. Vol. 29, No. 1. P. 163–196. URL: https://doi.org/10.1111/1467-6478.00215 (дата звернення: 05.08.2024).

160. Scott C. Analyzing Regulatory Space: Fragmented Resources and Institutional Design. Public Law. 2001. P. 329-353. URL: https://researchrepository.ucd.ie/handle/10197/7022 (дата звернення: 10.07.2024).

161. Group of Thirty. The Structure of Financial Supervision: Approaches and Challenges in a Global Marketplace. 2008. URL: https://group30.org/publications/detail/138 (дата звернення: 25.06.2024).

162. Borio C., Toniolo G. One Hundred and Thirty Years of Central Bank Cooperation: A BIS Perspective. BIS Working Papers No 197. 2008. URL: https://www.bis.org/publ/work197.pdf (дата звернення: 15.05.2024).

163. World Bank. Financial Sector Assessment Program (FSAP): Review of the 2017 Assessment. World Bank Group, 2017. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/265551513108465780/financial-sector-assessment-program-fsap-review-of-the-2017-assessment (дата звернення: 10.02.2024).

164. Про захист прав споживачів : Закон України від 12.05.1991 р. № 1023-XII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1023-12 (дата звернення: 15.01.2024).

165. Stiglitz J. E. Regulation and Failure. In New Perspectives on Regulation. The Tobin Project, 2010. P. 11-23. URL: https://tobinproject.org/sites/tobinproject.org/files/assets/New_Perspectives_Ch1_Stiglitz.pdf (дата звернення: 05.11.2024).

166. North D. C. Institutions, Institutional Change and Economic Performance. Cambridge University Press, 1990. URL: https://doi.org/10.1017/CBO9780511808678 (дата звернення: 10.10.2024).

167. Baldwin R., Black J. Really Responsive Regulation. The Modern Law Review. 2008. Vol. 71, No. 1. P. 59-94. URL: https://doi.org/10.1111/j.1468-2230.2008.00681.x (дата звернення: 15.09.2024).

168. Цивільний процесуальний кодекс України : Кодекс від 18.03.2004 р. № 1618-IV : станом на 1 бер. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 15.03.2024).

169. Господарський процесуальний кодекс України : Кодекс від 06.11.1991 р. № 1798-XII : станом на 1 бер. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1798-12 (дата звернення: 15.03.2024).

170. Кодекс адміністративного судочинства України : Кодекс від 06.07.2005 р. № 2747-IV : станом на 1 бер. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2747-15 (дата звернення: 15.03.2024).

171. Про виконавче провадження : Закон України від 02.06.2016 р. № 1404-VIII : станом на 1 лют. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1404-19 (дата звернення: 10.02.2024).

172. Coglianese C. Measuring Regulatory Performance: Evaluating the Impact of Regulation and Regulatory Policy. OECD Expert Paper No. 1. 2012. URL: https://www.oecd.org/gov/regulatory-policy/1_coglianese%20web.pdf (дата звернення: 15.01.2025).

173. Freistadt J., Suarez D. Legal Certainty in a Contemporary Context: Private and Criminal Law Perspectives. Springer, 2017. URL: https://doi.org/10.1007/978-981-10-3056-4 (дата звернення: 10.02.2025).

174. Warren E. Product Safety Regulation as a Model for Financial Services Regulation. Journal of Consumer Affairs. 2008. Vol. 42, No. 3. P. 452-460. URL: https://doi.org/10.1111/j.1745-6606.2008.00114.x (дата звернення: 05.01.2025).

175. Armour J., Awrey D., Davies P. et al. Principles of Financial Regulation. Oxford University Press, 2016. URL: https://doi.org/10.1093/acprof:oso/9780198786474.001.0001 (дата звернення: 15.12.2024).

176. Campbell-Verduyn M. Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance. Crime, Law and Social Change. 2018. Vol. 69, No. 2. P. 283-305. URL: https://doi.org/10.1007/s10611-017-9756-5 (дата звернення: 10.12.2024).

177. Blind K., Petersen S., Riillo C. The Impact of Standards and Regulation on Innovation in Uncertain Markets. Research Policy. 2017. Vol. 46, No. 1. P. 249-264. URL: https://doi.org/10.1016/j.respol.2016.11.003 (дата звернення: 05.12.2024).

178. Lodge M., Wegrich K. Crowdsourcing and Regulatory Reviews: A New Way of Challenging Red Tape in British Government?. Regulation & Governance. 2015. Vol. 9, No. 1. P. 30-46. URL: https://doi.org/10.1111/rego.12048 (дата звернення: 25.11.2024).

179. Reinhart C. M., Rogoff K. S. Financial and Sovereign Debt Crises: Some Lessons Learned and Those Forgotten. Journal of Banking and Financial Economics. 2014. Vol. 2, No. 4. P. 5-17. URL: https://doi.org/10.2139/ssrn.2387533 (дата звернення: 20.11.2024).

180. Ayres I., Braithwaite J. Responsive Regulation: Transcending the Deregulation Debate. Oxford University Press, 1992. URL: https://doi.org/10.1093/acprof:oso/9780195093766.001.0001 (дата звернення: 15.11.2024).

181. Pan E. J. Challenge of International Cooperation and Institutional Design in Financial Supervision: Beyond Transgovernmental Networks. Chicago Journal of International Law. 2011. Vol. 11, No. 1. P. 243-284. URL: https://chicagounbound.uchicago.edu/cjil/vol11/iss1/10/ (дата звернення: 10.11.2024).

182. Fenwick M., Kaal W. A., Vermeulen E. P. M. Regulation Tomorrow: What Happens When Technology Is Faster than the Law?. American University Business Law Review. 2017. Vol. 6, No. 3. P. 561-594. URL: https://digitalcommons.wcl.american.edu/aublr/vol6/iss3/1/ (дата звернення: 05.11.2024).

183. Brummer C. Disruptive Technology and Securities Regulation. Fordham Law Review. 2015. Vol. 84, No. 3. P. 977-1052. URL: https://ir.lawnet.fordham.edu/flr/vol84/iss3/4/ (дата звернення: 01.11.2024).

184. Coglianese C., Bennear L. S. Empirical Environmental Law Scholarship: A Survey of the Literature. In: Coglianese C., Segal D., Becker M. (eds.) Handbook of Environmental Law. Cambridge University Press, 2021. URL: https://doi.org/10.1017/9781108146623 (дата звернення: 25.10.2024).

185. Short J. L., Toffel M. W. Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment. Administrative Science Quarterly. 2010. Vol. 55, No. 3. P. 361-396. URL: https://doi.org/10.2189/asqu.2010.55.3.361 (дата звернення: 20.10.2024).