

<https://doi.org/10.15407/etet2024.04.005>

УДК: 336.74:004.9:330.322

JEL: D85, E42, E44, L86

Тетяна Кричевська

ПРОСТІР КРИПТОАКТИВІВ: ЛОГІКА РОЗВИТКУ, СТРУКТУРА, ВЛАСТИВОСТІ ТА ВЗАЄМОДІЇ

Стаття перша. Ідеологія, технології, шлях до розмаїття та типологія криптоактивів

Серія з двох статей присвячена з'ясуванню структури простору криптоактивів у його складності і розмаїтті, логіки його розбудови, особливостей взаємодії між його складовими та із зовнішнім світом. Показано, що відкритість кодів криптопроектів та поява різноманітних інструментів для спрощеного створення токенів на чужих блокчейнах перетворила простір криптоактивів на простір необмеженого створення фінансових активів. Структуру простору криптоактивів представлено за допомогою типології криптоактивів за технологічними, функціональними та соціально-економічними характеристиками. На основі вивчення тридцяти проектів криптоактивів з найбільшим обсягом капіталізації виявлено такі групи криптоактивів, що характеризують побудову криптопростору: біткоїн і етер як полюси розбудови криптопростору; альтернативні біткоїну платіжні криптоактиви; засновані на криптовалюти бек-офісні рішення для трансграничних платежів традиційного світу; стейблкоїни; криптоактиви альтернативних блокчейн-платформ з інноваційними механізмами консенсусу та іншими рішеннями масштабованості рівня 1 та рівня 2; криптоактиви проектів для масштабування інших блокчейнів, ефективною взаємодією блокчейнів між собою та із зовнішнім світом; криптоактиви проектів розбудови існуючих успішних віртуальних мереж; криптоактиви централізованих криптобірж; монети DeFi-проектів; мемні коїни; монети підвищеної конфіденційності; невзаємозамінні токени. Виявлено, що розбудова простору криптоактивів відбувається в таких напрямках: вирішення трилеми блокчейну з урахуванням цілей проекту; забезпечення інтероперабельності децентралізованих мереж; створення нових форм співпраці з традиційними фінансовими посередниками та іншими інституціями традиційного світу (що вже йде в розріз з ідеологією шифропанків). Обґрунтовано, що простір децентралізованих взаємодій, опосередковуваних криптоакти-

Кричевська Тетяна Олександрівна (tetyanakrychevska75@gmail.com), д-р екон. наук; провідний науковий співробітник Державної установи "Інститут економіки та прогнозування Національної академії наук України". ORCID: 0000-0003-1940-6820

Цитування: Кричевська Т. О. Простір криптоактивів: логіка розвитку, структура, властивості та взаємодії. Стаття перша. Ідеологія, технології, шлях до розмаїття та типологія криптоактивів. *Економічна теорія*. 2024. № 4. С. 5–28. <https://doi.org/10.15407/etet2024.04.005>

© Видавець Державна установа "Інститут економіки та прогнозування Національної академії наук України", 2024.
Стаття відкритого доступу за ліцензією CC BY-NC-ND 4.0
(<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.uk>)

вами, стає простором надвисокої волатильності, гіперфінансіалізації, простором, де важко відділити цінність технологій від спекулятивного ринку криптоактивів, де існують централізовані непрозорі і нерегульовані гіперпосередники, де відсутнє розмежування між професійними і непрофесійними учасниками крипторинку. Показано, що цей простір шукає додаткових джерел довіри у традиційному світі: через забезпечені суверенними валютами стейблкоїни; співпрацю з традиційними фінансовими посередниками та регуляторами, лобювання. У першій статті розглянуто ідеологічні засади, базові технології простору криптоактивів, біткоїн та етер як полюси розбудови цього простору та типологію криптоактивів.

Ключові слова: типологія криптоактивів, трилема блокчейну, блокчейн-платформа, необмежене створення фінансових активів, криптобіржа, децентралізовані фінанси.

THE CRYPTO-ASSET SPACE: DEVELOPMENT LOGIC, STRUCTURE, FEATURES, AND INTERACTIONS

ARTICLE 1. Ideology, technologies, the path to diversity, and the typology of crypto-assets

Tetiana Krychevska (tetyanakrychevska75@gmail.com), Doctor of Economics, Leading Researcher, State Organization "Institute for Economics and Forecasting of the National Academy of Sciences of Ukraine", Kyiv, Ukraine. OrcID: 0000-0003-1940-6820

The article explores the complexity and diversity of the crypto-asset space, examining the logic of its development, the dynamics of interactions within the ecosystem, and with the external world. It demonstrates how the open-source nature of crypto projects and the emergence of tools for simplified token creation on third-party blockchains have transformed the crypto-asset space into one of unlimited financial asset creation. The structure of the crypto-asset space is represented through a typology of crypto-assets based on technological, functional, and socio-economic characteristics. By studying thirty of the largest crypto-asset projects by market capitalization, several distinct groups that define the construction of crypto-asset space have been identified: bitcoin and ether as the poles of crypto space development; alternative to bitcoin payment cryptoassets; cryptocurrency based back-office solutions for traditional cross-border payments; stablecoins; coins of alternative blockchain platforms with innovative consensus mechanisms and scalability solutions (Layer 1 and Layer 2); crypto-assets of projects for scaling other blockchains and facilitating efficient interoperability between blockchains and the external world; crypto-assets of projects expanding existing successful virtual networks; crypto-assets of centralized cryptocurrency exchanges; DeFi project coins; meme coins; enhanced privacy coins; and non-fungible tokens (NFTs). The article reveals the ongoing development of the crypto-asset space in the following directions: solving the blockchain trilemma considering project goals; ensuring interoperability of decentralized networks; creating new forms of collaboration with traditional financial intermediaries and institutions (which often contrasts with the original cypherpunk ideology). It is argued that the space of decentralized interactions, mediated by crypto-assets, has become a domain of extreme volatility, hyper-financialization, and a space where it is difficult to separate technological value from speculative crypto markets. It also highlights the presence of centralized, opaque, and unregulated hyper-intermediaries, with no clear distinction between professional and non-professional participants in the crypto market. Furthermore, this space seeks additional sources of trust from the traditional world, including through sovereign currency-backed stablecoins, partnerships with traditional financial intermediaries, and regulatory lobbying. In the first article, the ideological foundations, basic technologies of the crypto-asset space, bitcoin and ether as the poles of development in this space, and the typology of crypto-assets are examined.

Keywords: typology of crypto-assets, blockchain trilemma, blockchain platform, unlimited creation of financial assets, cryptocurrency exchange, decentralized finance (DeFi).

Біткоїн задумувався і сприймався як інноваційна форма грошей і платіжної системи, тож протягом першого десятиріччя від його появи дослідники намагалися визначити місце криптовалюти у таксономії грошей (*Virtual Currencies*, 2016; *Bech, Garratt*, 2017). Макроекономічні дослідження, з огляду на те, що здебільшого вартість криптовалют коливалася синхронно з ціною біткоіна, часто розглядають простір криптоактивів як єдине ціле, досліджуючи кореляцію курсу біткоіна з різними макроекономічними показниками: інфляцією, індексами фондового ринку, курсом долара США та ін. (*Corbet et al.*, 2018; *Bouri et al.*, 2017; *Guesmi et al.*, 2019; *Nguyen*, 2022; *Мищенко та ін.*, 2022). Але з часом сфера криптовалют до такої міри розширилася й ускладнилася, що експерти та регулятори переходять від поняття криптовалюти до більш широких понять *віртуального активу і криптоактиву*. У Регламенті ЄС "Про ринок криптоактивів" 2023/1114 від 31 травня 2023 р. криптоактив визначається як "цифрове представлення цінності або прав, які можуть переказуватися та зберігатися в електронному вигляді за допомогою технології розподіленого реєстру або подібної технології"¹. Технологія розподіленого реєстру (TPP) є архітектурою бази даних, яка дозволяє зберігати і обмінюватися записами у розподілений і децентралізований спосіб, забезпечуючи їхню цілісність за допомогою використання протоколів перевірки на основі консенсусу і криптографічних підписів (*Venos et al.*, 2017, *Кричевська*, 2018b).

До різних частин простору криптоактивів уже починають застосовувати різні підходи у регулюванні: одні можуть регулювати як електронні гроші, другі – як фінансові інструменти, треті – згідно зі спеціально розробленими нормами, четверті – визнати незаконними; те саме стосується розуміння природи та регулювання постачальників послуг, пов'язаних із криптоактивами.

Стаття присвячена з'ясуванню структури простору криптоактивів у його складності і розмаїтті, логіки його розбудови, особливостей взаємодії між його складовими та із зовнішнім світом. Для цього запропоновано розширену типологію криптоактивів за технологічними, функціональними та соціально-економічними характеристиками та "топографію криптопростору" – з'ясування особливостей та видів проєктів, пов'язаних із 30 криптоактивами з найбільшим обсягом капіталізації. У першій статті буде розглянуто ідеологічні засади, базові технології простору криптоактивів, біткоїн та етер як полюси розбудови цього простору та типологію криптоактивів.

Ідеологічні засади простору криптоактивів. Сучасні технології пропонують людині чимало можливостей для спілкування без кордонів і досвіду без кордонів, але паралельно зі зростанням можливості порівняти власне життя з життям людей у найвіддаленіших куточках світу зростає нерівність й усвідомлення інституційних обмежень для самореалізації

¹ On markets in crypto-assets. Regulation (EU) 2023/1114 of the European Parliament and of the Council (2023). May 31. EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

(Гриценко, 2022). Шумпетерівський процес творчого руйнування передбачає знаходження нових можливостей в існуючому інституційному просторі. Поява ж простору криптоактивів, в якому цінність може створюватися, передаватися і зберігатися без захисту, гарантій і обмежень з боку системи інститутів, винесла інноваційний процес на інший рівень, де правила і стимули вибудовуються "з чистого аркуша". Символічно, що концепції і технологічні рішення проєктів у криптопросторі оприлюднюються у Білих книгах (White Paper). Звісно, це породжує ризики, що система, вибудовуючи алгоритми і стимули, буде наново через кризи проходити шлях становлення традиційних інститутів, бо їй доведеться мати справу з тією самою людською природою, і що злочинці першими скористаються можливостями "чистого аркуша". А втім, це захопливе поле для тестування нових організаційних форм людських взаємодій.

Ідеологію і технологію, покладені в основу біткоіна та наступних криптоактивів, було розроблено представниками руху шифропанків – активістів, які виступають за захист приватності та свободи через використання криптографії та децентралізованих технологій. Цей рух постав у 1990-х рр. як реакція на зростаючий контроль урядів і корпорацій над інформацією та особистими даними користувачів в Інтернеті. Ось, скажімо, бачення цього нового світу В. Дая, який у 1998 р. запропонував одну з перших концепцій децентралізованої цифрової валюти b-money. [Криптоанархія – це] "спільнота, де ... насилля неможливе, бо її [спільноти] учасників не можна пов'язати з їхніми справжніми іменами чи фізичними місцями розташування". "...Ефективна співпраця вимагає засобу обміну (грошей) та способу забезпечення виконання контрактів" (Dai, 1998). Власне, простір криптоактивів і намагається вирішити ці два завдання – спочатку виник перший децентралізований віртуальний платіжний засіб, що спирався на технології криптографії і розподіленого реєстру, – біткоїн, потім Ethereum – перша блокчейн-платформа, середовище, де можна створювати і запускати контракти, виконання яких не потребує участі посередників, які гарантують права учасників. Практика використання цих інструментів виявила численні їхні обмеження. Почала навіть формуватися теорія цього криптопростору: у 2017 р. засновником Ethereum В. Бутерінім було сформульовано "трилему блокчейну" про неможливість одночасного досягнення в блокчейні *децентралізації, масштабованості і безпеки* (Sharding FAQ, 2017). Кожен блокчейн, намагаючись покращити один із цих аспектів, змушений жертвувати іншим. Тож розбудова простору криптоактивів відбувалася як пропозиція різних варіантів вирішення цієї трилеми залежно від цілей проєкту. Зараз простір криптоактивів налічує десятки тисяч коїнів та токенів. Навколо багатьох з них створені цілі екосистеми, і вони вибудовують шляхи взаємодії. Знайомство з побудовою простору криптоактивів розпочнемо з біткоіна та етеру, які стали відправними точками для нових проєктів, що удосконалювали або доповнювали їхній функціонал.

Біткоїн та етер як полюси розбудови простору криптоактивів.

Біткоїн. Які технологічні рішення лежать в основі біткоїна? По-перше, реєстрація користувачів і перевірка паролів без центрального сервера здійснюються за допомогою *криптографії відкритого ключа* (ключ, який використовується для розшифрування повідомлення, не збігається з ключем, який використовується для його шифрування). Цей метод у 1976 р. запропонували В. Діффі та М. Геллман у роботі "Нові напрямки в криптографії" для безпечного зв'язку через відкриті канали (*Diffie, Hellman, 1976*). До 1990-х рр. більшість криптографічних алгоритмів були або комерційними, або використовувалися урядами. Уряд США класифікував сильну криптографію як "боєприпаси" (munitions) з міркувань національної безпеки, що обмежувало її експорт (*Mehta et al., 2021*). Автор ефективного та доступного методу шифрування PGP (Pretty Good Privacy) Ф. Циммерман обійшов це обмеження, скориставшись Першою поправкою до Конституції США, яка захищає свободу слова і друку, – опублікував вихідний код PGP у вигляді книги (*Levy, 2002*).

По-друге, для уникнення подвійного витрачання без третьої сторони, що веде централізований реєстр платежів, використовується механізм ведення реєстру і узгодження порядку платежів усіма учасниками мережі (*розподілений реєстр*). Синхронізація порядку транзакцій ускладнюється тим, що на швидкість і порядок отримання транзакцій різними вузлами впливають географія, технології, можливості підключення, пропускна спроможність і т. п. Аби полегшити процес узгодження порядку транзакцій, їх додають до реєстру не по одній, а пакетами, що дістали назву блоків. Тож замість узгоджувати порядок транзакцій, валідатори (вузли, що підтверджують правомірність транзакцій), узгоджують порядок блоків, які генеруються рідше. По-третьє, для того щоб гарантувати *добросесність валідаторів*, які формують блоки, система передбачає здійснення ними витрат на генерацію блоку, тоді включення до блоку неправомірних транзакцій приведе до відкидання блоку іншими валідаторами і відповідних збитків. Цей механізм консенсусу дістав назву *Proof of Work (PoW) – Доказ роботи*. Для створення нових блоків відповідні учасники мережі повинні розв'язувати криптографічні задачі, що вимагають використання енергії та обчислювальних потужностей. Цю технологію запропонували у 1992 р. С. Дворк і М. Наор у статті "Ціноутворення через обчислення або боротьба зі спамом" (*Dwork, Naor, 1993*) для скорочення кількості небажаної пошти. По-четверте, оскільки формуванням блоків транзакцій займаються багато учасників² одночасно, потрібно вирішити, чий блок додати до реєстру. В межах механізму доказу роботи переможцем стає учасник, який вперше розв'язав криптографічну задачу. Для генерації унікальної часової мітки –

² Термін "майнери" (miners – ті, що займаються видобутком корисних копалин) не використовується у Білій книзі біткоїна. Ідея порівняння біткоїна із золотом – як форми "цифрового золота" – з'явилася пізніше, десь у 2011–2012 рр., коли біткоїн почали порівнювати із золотом через його обмежену пропозицію (максимально 21 мільйон біткоїнів), зростаючу вартість та роль як засобу заощадження.

хешу блоку – використовують три типи вхідних даних: хеш останнього блоку, транзакції та спеціальний номер – *nonce* (number used only once), який обирає учасник. Переможцем стає той, хто, перебираючи різні значення *nonce*, із цих вхідних даних першим згенерує значення хеш-функції, що починається з певної кількості нулів.

Як відомо, система біткоіна передбачає зростання його пропозиції спадними темпами до досягнення 21 млн. Проте код біткоіна був відкритим – його можна було копіювати і створювати нові блокчейни та нові криптовалюти. *Це відкривало більш широкі можливості для створення фінансових активів, ніж у традиційному світі, але потребувало технічних знань. Тоді почали з'являтися ініціативи, що пропонували простіші способи створення нових криптоактивів на чужих блокчейнах.*

Подібні проєкти почали реалізовуватися навіть до появи у 2015 р. адаптованої для цього блокчейн-платформи Ethereum, – на блокчейні біткоіна, хоча він свідомо не розрахований для широкого функціоналу (його простота мала сприяти безпеці). У 2012 р. було запущено проєкт Colored Coins, який давав можливість "розфарбовувати" біткоіни криптографічними позначками для створення нових активів. У липні 2013 р. було запущено протокол *Mastercoin* (зараз *Omni Layer*), який використовував блокчейн Bitcoin для реєстрації та перевірки транзакцій з іншими активами, крім самого BTC. *Omni* дозволяє створювати свої власні токени і проводити транзакції з ними, а також розгорнути прості смарт-контракти. *Omni Layer* додає додаткову інформацію до стандартних транзакцій у блокчейні Bitcoin через поле *OP_RETURN*, яке використовується для зберігання даних у блокчейні. Інтерпретація цих даних здійснюється програмним забезпеченням *Omni*, яке розуміє структуру цих додаткових полів. Тобто сам блокчейн біткоіна залишається незмінним, а *Omni* додає функціональність через цей "накладений" рівень. Так з'явилися *криптокотени* – криптоактиви, що існують як елемент програмного коду на базі вже існуючого блокчейну, який забезпечує його технічну і економічну функціональність. Один із найвідоміших токенів, випущених через *Omni Layer*, – це найпоширеніший на сьогодні стейблкоїн *Tether (USDT)*.

Етер. У 2013 р. було оприлюднено розроблену канадійським вченим-комп'ютерником В. Бутерінім Білу книгу *Ethereum*, у 2014 р. розроблену англійським вченим Г. Вудом Жовту книгу (*Yellow Paper*) *Ethereum* – технічний документ, а в 2015 р. запущено блокчейн першої блокчейн-платформи – середовища, яке дає змогу децентралізувати не лише платежі, але й інші види взаємодій. Платформа дістала назву від терміна *ether*, яким раніше називали гіпотетичну субстанцію, що проникала в усі простори і вважалася носієм світла. У блокчейні Ethereum можна надсилати транзакції, які створюють *смарт-контракти* – комп'ютерні алгоритми, що забезпечують автоматичне виконання контрактів у середовищі блокчейну у разі настання передбачених умов. Концепція смарт-контрактів була запропонована американським інформатиком і криптографом Н. Сабо у 1996 р.: "Нові інституції та нові способи формалізації відносин, що скла-

дають ці інституції, тепер стали можливими завдяки цифровій революції. Я називаю ці нові контракти «розумними», бо вони набагато функціональніші від своїх бездушних паперових предків. Жодного використання штучного інтелекту для цього не передбачається. Розумний контракт – це набір обіцянок, визначених у цифровій формі, включно з протоколами, в межах яких сторони виконують ці обіцянки" (Szabo, 1996).

Отже, особливість Ethereum полягає в тому, що в блокчейні здійснюється більше типів транзакцій. Різні типи транзакцій мають різну обчислювальну складність. Наприклад, транзакція, яка виконує простий платіж в ETH – криптоактиві проєкту, менш складна, ніж транзакція із завантаження або запуску смарт-контракту. Через це в Ethereum існує концепція "газу" – одиниць обчислювальної складності різних типів операцій, які ви доручаєте майнерам виконати у вашій транзакції. Отож, плата ініціатора транзакції за майнінг становитиме добуток обсягу спожитого газу на ціну газу (ETH за одиницю газу), яку він готовий заплатити. Надсилаючи транзакцію в Ethereum, ви вказуєте ціну газу та ліміт газу (максимальна кількість газу, яку ви дозволите використовувати в транзакції), бо наперед неможливо точно визначити, скільки обчислювальних ресурсів потребуватиме здійснення транзакції (Lewis, 2018).

Проблема смарт-контрактів полягає в тому, що вони не є ані розумними (здатними адаптуватися до несподіваних ситуацій), ані контрактами (не мають юридичної сили, спірні ситуації не можуть бути вирішені в суді) (Werbach, Cornell, 2017; De Filippi, Wright, 2018). Утім, це обмеження не перешкоджало їхньому використанню для створення інших криптоактивів на блокчейні Ethereum.

У 2017 р. почалася нова ера в історії криптовалют як надзвичайно волатильного спекулятивного фінансового активу, коли вартість біткоїна зросла з менше 1 тис. дол. США в кінці 2016 р. до понад 19 тис. дол. в кінці 2017 р. Відправною точкою цієї нової ери став бум ICO (Initial Coin Offering). ICO – це механізм залучення коштів шляхом продажу інвесторам криптовалютних токенів, які можуть виконувати різні функції: бути засобом обміну, внутрішньою валютою платформи, надавати право голосу, надавати у майбутньому доступ (чи пільговий доступ) до певних послуг чи продукції, що виробляються емітентом. Це стало можливим завдяки появі першого стандарту токенів для Ethereum – ERC-20, який визначає набір правил і функцій, які токен повинен мати для сумісності з іншими смарт-контрактами та платформами, наприклад, гаманцями або біржами. Стандарт, який значно спростило створення нових токенів, було запропоновано Ф. Вогельштеллером і затверджено спільнотою Ethereum у листопаді 2015 р. в межах Ethereum Improvement Proposals (EIP) – постійно-діючого механізму для пропонування змін, удосконалень і нових стандартів мережі. Приверненню масової уваги до фінансування проєктів за рахунок ICO сприяв й інцидент зі зламом і викраденням коштів зі смарт-контракту "The DAO" – криптовалютного фонду для фінансування стартапів, оскільки він зрештою спричинив розгалуження блокчейну Ethereum. Першими можли-

вістю легкого залучення коштів через ICO скористалися ті, хто не планував реалізовувати проекти у криптосфері – згідно зі звітом, підготовленим для Bloomberg аналітичною компанією SATIS Group, 78 % проектів ICO під час буму 2017 р. виявилися шахрайськими (Delisle, 2018).

Утім, відтоді було реалізовано і численні життєздатні криптопроекти, які пропонували таке: нові варіанти платіжних криптоактивів – альтернативи біткоїну (з вищою масштабованістю, нижчими комісійними, більшою анонімністю, адаптацією до регуляторних вимог певних юрисдикцій і т.п.); альтернативні Ethereum блокчейн-платформи; інструменти забезпечення сумісності і взаємодії між блокчейнами, інструменти удосконалення взаємодій блокчейнів з даними зовнішнього світу; фінансові проекти на блокчейні (біржі, криптокредитори і т.п.). Як наслідок, сьогодні існують десятки тисяч криптоактивів і токенів з найрізноманітнішими технічними характеристиками і функціями, що надають їм тієї чи іншої природи.

У межах трилеми блокчейна Ethereum робить вибір на користь високої безпеки та децентралізації, жертвуючи масштабованістю. Пропускна здатність платформи становить лише 15–30 транзакцій на секунду (TPS), а комісійні, особливо під час піків навантаження, можуть бути досить високими. У майбутньому Етеріум планує запровадити ряд рішень масштабованості рівня 1, таких як шардинг (про нього див. нижче), що теоретично може збільшити TPS Етеріуму до тисяч. Запровадження цих модифікацій блокчейну потребує часу, а поки що проблему масштабованості вирішують розробники інших, сторонніх проектів, пропонуючи клієнтам різні рішення рівня 2 (Layer 2) (див. нижче) для прискорення і здешевлення їхніх транзакцій на самому Ethereum, та розробники альтернативних блокчейн-платформ, що пропонують нові рішення проблеми масштабованості вже на рівні 1.

Типологія криптоактивів. Науковцями, регуляторами та міжнародними фінансовими організаціями запропоновано численні підходи до типології криптоактивів. Спираючись на існуючі класифікації (Garrido, 2023; Freni et al., 2022; Coelho et al., 2021; Euler, 2018) та вивчення специфіки функціонуючих екосистем криптоактивів, ми пропонуємо класифікувати криптоактиви за трьома групами характеристик: *технологічні, функціональні та соціально-економічні*.

1. Технологічні характеристики описують технічні аспекти криптоактивів, пов'язані з тим, як вони функціонують на рівні блокчейну та інших технологій. Ці характеристики визначають, як саме конструкція криптоактиву вирішує проблеми безпеки, децентралізації, швидкості і вартості транзакцій, інтероперабельності з іншими віртуальними просторами і традиційним світом.

До них можна віднести:

1.1. Різновид TPP, що лежить в основі криптоактиву (Goldman, Kumar, 2021). Блокчейн – дані зберігаються у вигляді послідовних блоків, що з'єднані між собою в ланцюг. Кожен блок містить список транзакцій і

унікальний хеш попереднього блоку, що забезпечує його цілісність (*біткоїн, етер і більшість криптоактивів*). *Спрямований ациклічний граф (DAG – Directed Acyclic Graph)* – дані розміщуються не в блоках, а у вигляді графа, де кожна нова транзакція підтверджує одну або кілька попередніх. Це дозволяє системі масштабуватися більш ефективно, особливо для мікротранзакцій (*Kaspa, IOTA, Nano*). *Hashgraph* поєднує DAG з інноваційним механізмом "пліток про плітки" (*Gossip About Gossip*): кожен вузол не лише передає інформацію про нову транзакцію, а й включає мета-інформацію про те, як він отримав ці дані (тобто про які події йому "розказали" інші вузли). Це дозволяє всім вузлам бачити повну історію взаємодії між учасниками мережі і досягати консенсусу без голосування (*Hedera Hashgraph*). TRP постійно розвиваються, виникають нові її різновиди: *Holochain, Tempo*, гібридні види (*Dutta, 2022*).

1.2. Механізми консенсусу в блокчейні, з яким пов'язаний криптоактив. Вище ми описали історично перший механізм консенсусу *Proof of Work (PoW) – Доказ роботи*. Окрім біткоїна, він використовується також *Litecoin, Bitcoin Cash, Ethereum Classic, Ethereum* до переходу на Proof of Stake у 2022 р. PoW надає високий рівень безпеки, але пов'язаний зі значними енергетичними витратами та має обмежену масштабованість. Попри застереження творця біткоїна під псевдонімом Сатоші Накомото, майнери в гонитві за винагородою включилися у перегони майнінгової потужності, що призвело до зростання хешрейту системи – сукупної кількості хешів (спроб знайти хеш, який дає право додати блок до блокчейну), які виконуються всіма майнерами в мережі за одну секунду, з 23,1 терахешів (трильйонів хешів) на секунду в кінці 2012 р. до 665 ексахешів (квінтільйонів, тобто 10^{18}) на секунду 13 жовтня 2024 р.³.

Proof of Stake (PoS) – Доказ володіння часткою. Імовірність обрання валідатора для створення блоку залежить від кількості криптоактивів, які вони «заставляють» або блокують. Протокол блокчейну може передбачати конфіскацію застави у разі недоброчесної поведінки відповідного учасника мережі (*Ethereum 2.0, Cardano, Polkadot, BNB* та багато ін.).

Delegated Proof of Stake (DPoS) – Делегований доказ частки. DPoS є модифікацією PoS, де власники токенів голосують за делегатів, які представляють їхні інтереси і перевіряють транзакції. Делегати обираються для створення блоків і отримують винагороду. Цей механізм прискорює досягнення консенсусу, але передбачає централізацію (*EOS, Tron*).

Proof of Authority (PoA) – Доказ авторитету. Учасники, які хочуть стати валідаторами, проходять процес перевірки та затвердження. Використовується у приватних або корпоративних блокчейнах, де децентралізація не є основним пріоритетом (*VeChain* – блокчейн-платформа, розроблена для покращення управління ланцюгами постачання та інших бізнес-процесів).

³ Bitcoin Hashrate Chart. *CoinWarz*.
URL: <https://www.coinwarz.com/mining/bitcoin/hashrate-chart>
ISSN 1811-3141. *Економічна теорія*. 2024. № 4

Proof-of-Capacity (PoC) – Доказ потужностей. Майнери створюють і зберігають великі набори даних (так звані "плот-файли") на своєму диску. Ці файли містять попередньо обчислені значення хешів, які будуть використовуватися для знаходження правильного блоку. Під час майнінгу блокчейн надсилає майнерам запит, і вони використовують дані зі своїх плот-файлів, щоб знайти значення хеш-функції, яке задовольняє умовам задачі. Чим більше дискового простору використовується для зберігання плотів, тим більше шансів у майнера знайти правильне рішення і отримати винагороду (*Filecoin, Internet Computer, BitTorrent*).

Proof of History (PoH) – Доказ історії. Це унікальний механізм, впроваджений у мережі *Solana* у поєднанні і для прискорення PoS. PoH дозволяє створювати часові мітки на транзакціях відразу після їх надсилання та впорядковувати транзакції незалежно від валідаторів, що значно скорочує час, потрібний для перевірки та додавання нових блоків.

Byzantine Fault Tolerance (BFT) – Протоколи візантійської стійкості. Це група механізмів досягнення консенсусу шляхом проведення кількох раундів опитувань валідаторами один одного, що забезпечує добросовісність мережі навіть за наявності до третини недобросовісних валідаторів (*Aptos, Stellar, Ripple*).

Це далеко не вичерпаний перелік механізмів консенсусу, але він ілюструє різні підходи до вирішення трилеми блокчейну.

1.3. Відкритість блокчейну. *Відкритий блокчейн* – де всі користувачі можуть брати участь у консенсусі і перевіряти транзакції (*Bitcoin, Ethereum*). *Приватний блокчейн* – права доступу контролюються централізовано, використовується для корпоративних цілей (наприклад, *Hyperledger Fabric*). *Консорціумний блокчейн* керується групою організацій, які спільно приймають рішення. Прикладом є *Corda* – технологічна платформа на основі TRP, створена консорціумом R3, який об'єднує понад 200 фінансових установ, компаній та державних установ з усього світу – розроблена для полегшення проведення угод і співпраці між різними учасниками в бізнесі, з акцентом на дотримання конфіденційності та забезпечення високої продуктивності. Найбільше використовується у фінансовій сфері та сфері державних послуг. Один із найвідоміших проєктів, побудованих на *Corda*, це *Contour*, що оптимізує обробку документарних акредитивів у міжнародній торгівлі. Учасники, такі як HSBC, ING та Standard Chartered, використовують його для зменшення часу на обробку угод з кількох тижнів до кількох днів. У Швеції та Індії технологія *Corda* тестується для ведення реєстрів земельних ділянок, у Великій Британії – для випуску цифрових облігацій).

1.4. Місце криптоактиву у технологічному стеку блокчейну. *Нативний (власний) криптоактив* блокчейну створюється разом із відповідним блокчейном і необхідний для функціонування інфраструктури та протоколу консенсусу). Серед них виокремлюють такі види: новий ланцюг, новий код (*Bitcoin, Ethereum*); новий блокчейн, розгалужений код – криптоактиви нових блокчейнів, які копіюють кодову базу існуючого блокчейну, змінюючи деякі параметри (*Litecoin, Dogecoin, ZCash*); розгалужений блок-

чейн, розгалужений код – криптовалюта блокчейну, який виникає в результаті "хард-форку" (*Ethereum Classic, Bitcoin Cash*); криптоактиви додатків, розміщених на чужому блокчейні (*Freni et al., 2022*) (крип토포кени – *Tether (USDT), Chainlink (LINK), USD Coin (USDC) Maker (MKR), Basic Attention Token (BAT), Uniswap (UNI)*).

1.5. Методи масштабування у блокчейні, з яким пов'язаний криптоактив. Масштабування блокчейну – це вирішення проблеми обмеженої пропускнуої здатності (транзакцій на секунду), яка виникає через децентралізовану природу блокчейнів. Вибір певного методу, згідно з трилемою блокчейну, водночас впливає і на інші характеристики блокчейну.

Перша група цих методів – у межах блокчейну – це способи, які безпосередньо змінюють основний протокол блокчейну, щоб підвищити його масштабованість. *Збільшення розміру блоку* прискорює транзакції, збільшуючи їхню кількість, яка може вміститися в одному блоці. Bitcoin Cash збільшив розмір блоку до 8, а потім до 32 МБ, порівняно з 1 МБ у Bitcoin. Недоліком є підвищення вимог до зберігання та обчислювальних потужностей, що посилює централізацію мережі. *Шардинг* (sharding) – метод горизонтального розділення блокчейну на окремі частини, які називаються "шардами". Кожен шард обробляє частину транзакцій паралельно з іншими шардами. Завдяки цьому мережа може збільшувати кількість транзакцій, оброблених одночасно, не перевантажуючи один глобальний блокчейн. Усі шарди працюють незалежно, але періодично синхронізуються для підтримки загальної цілісності мережі. Проблема зменшення кількості валідаторів кожної транзакції може вирішуватися, скажімо, шляхом призначення валідаторів на різні шарди у випадковий спосіб, що обмежує можливості змови. Ethereum планує впровадити шардинг у межах Ethereum 2.0. Перевагою є значне підвищення пропускнуої здатності без збільшення вимог до окремих вузлів, а недоліками – складність реалізації та можливі проблеми з безпекою під час обміну інформацією між шардами. Ще один метод масштабування – це власне *зміна або модифікація алгоритму консенсусу* (як-от перехід Ethereum з PoW на PoS). Перевагою є радикальна зміна властивостей блокчейну, але такі значні зміни у протоколі вже діючого великого проєкту не завжди легко реалізувати. *Стиснення даних* – видалення або архівація старих даних, що зменшує розмір блокчейну. Прикладом є технологія *SegWit (Segregated Witness)*, запроваджена у Bitcoin та Litecoin: цифрові підписи (witness) відокремлюються від основних даних транзакції і виносяться в окрему частину блоку, що дозволяє помістити до блоку більше транзакцій. Зокрема, у мережі Біткоїн максимально можливий ефективний розмір блоку завдяки цьому зріс з 1 до 4 Мб (на практиці часто коливається між 1 і 2 Мб). Недоліком цього рішення може бути ускладнення доступу до історичних даних.

Друга група методів масштабування – так звані *рішення другого рівня (Layer 2)*. Вони працюють поверх основного блокчейну, і використовують його лише для підтвердження основних транзакцій.

Платіжні канали (Payment Channels) – технологія, яка дозволяє двом або більше сторонам проводити транзакції поза основним блокчейном з можливістю остаточного запису результатів транзакцій у блокчейн після завершення. На блокчейні створюється мультипідписний гаманець, де блокується певна кількість криптовалюти. Учасники можуть обмінюватися підписаними транзакціями, які оновлюють баланс гаманця поза блокчейном. Ці транзакції не транслюються в блокчейн одразу. Коли одна зі сторін бажає завершити взаємодію, останній стан балансу транслюється в блокчейн, і кошти розподіляються відповідно до цього стану (канал закривається) (*Lightning Network* у Bitcoin і Litecoin).

Ролупи (Rollups – згортки) – технологія, що передбачає обробку транзакцій поза основним блокчейном, потім "згортання" великої кількості транзакцій в одну, і в такому стисненому вигляді їх запис на основному блокчейні, причому так, що він все одно гарантує їхню валідність. *ZK-Rollups* використовують криптографічні докази нульового розголошення (*Zero-Knowledge Proofs*) для підтвердження правильності транзакцій. Доказ з нульовим розголошенням – це криптографічний метод, за допомогою якого одна сторона може довести іншій, що вона знає деяку інформацію, не розкриваючи самої інформації. У випадку криптографії з відкритим ключем ви передаєте зашифровану відповідь і кажете, що її можна розшифрувати вашим відкритим ключем. У випадку доказу з нульовим розголошенням ви показуєте, що знаєте відповідь, але не кажете, якою саме є відповідь. Ви виконуєте дії, що переконують іншого, що ви знаєте правильну відповідь, не розкриваючи її. Тож ZKP забезпечує більшу конфіденційність, оскільки секретна інформація не передається і не використовується відкритий ключ для перевірки. Ідею цієї технології можна пояснити на такому прикладі. Нехай є лабіринт із двома виходами і замкненими дверима між ними, які можна відчинити тільки за допомогою спеціального коду. Ви хочете довести, що маєте цей код, але не хочете розкривати сам код. Ви заходите в лабіринт і обираєте будь-який маршрут. Верифікатор не знає, який шлях ви обрали, але може наказати вам вийти з лабіринту через будь-які двері. Якщо ви знаєте код, ви завжди зможете відкрити будь-які двері і вийти через них. Верифікатор бачить, що ви щоразу виходите через потрібні двері, і доходить висновку, що ви справді знаєте код. *Оптимістичні ролупи (Optimistic Rollups)* обробляють транзакції "оптимістично", тобто припускають, що всі транзакції дійсні, і лише потім перевіряють їх, якщо виникає суперечка або сумнів. Після того, як блок із транзакціями передано на основний ланцюг, є певний період часу, протягом якого будь-хто може оскаржити транзакцію, яка в цьому разі верифікується. Якщо транзакція виявляється неправомірною, блок відхиляється, і особа, яка оскаржила транзакцію, отримує винагороду за виявлення помилки. Якщо ж транзакція виявляється добросовісною, то цей вузол втрачає свою заставу.

Сайдчейни (Sidechains) – це окремі блокчейни, що працюють паралельно з основним блокчейном. Вони мають власні механізми консенсусу і підключені до основного ланцюга через двосторонній міст. Активи пере-

даються з основного ланцюга на сайдчейн через мости і можуть бути повернуті назад у будь-який момент. Перевагою цього механізму масштабування є гнучкість – розробники можуть впроваджувати різні правила або функції на сайдчейні, а слабким місцем може стати безпека (сайдчейни мають власні моделі безпеки, мости можуть бути вразливими для атак, бо не є децентралізованими системами) і складність управління взаємодією між основним ланцюгом і сайдчейнами.

1.6. Можливість використання криптоактиву на різних блокчейнах. За цим критерієм виділяють одночейнові та мультичейнові криптоактиви. До технологій, які дозволяють створювати мультичейнові токени, можна віднести, передусім, стандарти токенів: ERC-20 (Ethereum), TRC-20 (TRON), ASA (Algorand), SPL (Solana) та ін. Використовуючи такі стандарти, стейблкоїн Tether існує на різних платформах. Друга технологія – *міжчейнові мости*. Мости дозволяють переказувати активи між різними блокчейнами за допомогою блокування оригінальних токенів на вихідному ланцюгу і створення загорнутих токенів на цільовому блокчейні. Оригінальний криптоактив зберігається в спеціальному сховищі або смарт-контракті на початковому блокчейні. На основі цього депонованого активу випускається токен на іншому блокчейні, наприклад, на Ethereum. Цей токен називається "загорнутим" (wrapped) і має таку ж цінність, як і оригінальний актив. Власник загорнутого активу може в будь-який момент обміняти його на оригінальний актив, використовуючи процедуру "розгортання" (unwrap). Прикладами загорнутих токенів є: *Wrapped Bitcoin (WBTC)* – загорнутий біткоїн на блокчейні Ethereum, що дає змогу використовувати BTC в екосистемі Ethereum, зокрема у децентралізованих фінансах (DeFi); *Wrapped Ethereum (WETH)* – загорнутий ETH на блокчейні Ethereum, що надає можливість використовувати Ethereum у стандартах ERC-20, оскільки ETH сам по собі не є токеном ERC-20; *Wrapped Binance Coin (WBNB)* – загорнутий Binance Coin (BNB) на блокчейні Ethereum; *RenBTC*, що дозволяє використовувати біткоїн у різних блокчейн-екосистемах через децентралізовану мережу Ren; *Wrapped Polkadot (WPolkadot)* – загорнутий токен Polkadot (DOT) на Ethereum; *Wrapped XRP (WXRP)* – загорнутий токен XRP на блокчейні Ethereum та ін. Ще однією технологією емісії мультичейнових токенів є *мультичейнові стандарти токенів*, які дозволяють функціонування токена на кількох блокчейнах без необхідності створення загорнутих версій. Наприклад, стандарт ERC-20 в Ethereum може бути адаптований для інших блокчейнів, але для цього потрібні додаткові механізми взаємодії. Інші стандарти, як-от Polkadot's XCMP (Cross-chain Message Passing) чи Cosmos IBC (Inter-Blockchain Communication), дозволяють токенам пересуватися між блокчейнами без зміни їхньої суті. Наприклад, нативний криптоактив мережі Polkadot – DOT використовує стандарт XCMP (Cross-chain Message Passing), що дозволяє токенам нативно переміщуватися між парачейнами екосистеми Polkadot.

1.7. Взаємозамінність. Така характеристика з'явилася з появою *non-fungible token (NFT)* – цифрових елементів на основі блокчейну, оди-

ниці яких спроектовані так, щоб бути унікальними. Дані, які зберігаються в NFT, можуть бути пов'язані з зображеннями, відео, аудіо, фізичними об'єктами, членством та ін. NFT були винайдені в 2014 р. підприємцем А. Дашем і художником К. Маккоєм для засвідчення, що предмет є цифровим оригіналом (Dash, 2021). Отже, за цим критерієм криптоактиви поділяються на взаємозамінні і невзаємозамінні.

1.8. Анонімність. За цим критерієм можна виділити *псевдонімні* та *анонімні* криптоактиви. Транзакції у *псевдонімних* криптоактивах можуть бути відстежені і мають певний рівень прозорості (*біткоїн, етер*). *Анонімні* криптоактиви пропонують високий ступінь анонімності транзакцій за допомогою використання технології Zero-knowledge Proofs, про яку йшлося вище (*Zcash (ZEC)* у такий спосіб приховує відправника, отримувача та суму транзакції); технології кільцевих підписів та одноразових адрес (*Monero* – про цей проєкт йтиметься детальніше у другій статті цієї серії), створення приватних блокчейнів всередині публічного блокчейна (*Horizen*); змішування монет відправника з монетами інших користувачів (*Dash*), об'єднання декількох транзакцій (*Dash*) та ін.

2. Функціональні характеристики описують роль і призначення криптоактиву в екосистемі: для проведення платежів, участі в управлінні проєктом, отримання доступу до послуг або ресурсів і т. д.

2.1. Платіжні криптоактиви призначені передусім для виконання функцій грошей, що визначає специфіку відповідних блокчейнів, які мають меншу функціональність, але більшу безпеку і децентралізацію (*Bitcoin, Litecoin, Bitcoin Cash, Kaspa*). Інша річ, що в процесі розвитку екосистеми криптоактивів вони стали переважно використовуватися як фінансові активи.

2.2. Токени цінних паперів передбачають такі самі права власника, як і цінні папери, тому їхня емісія і операції з ними регулюються національними та наднаціональними (такими як MIFID II – Директива про ринки фінансових інструментів у ЄС) правовими актами щодо цінних паперів. У США для встановлення відповідності токенів критеріям "інвестиційного контракту" використовується тест Хоуї – критерії, вироблені Верховним судом США у 1946 р. на основі судового прецеденту у справі SEC проти W. J. Howe Co. Інструмент кваліфікується як інвестиційний контракт, якщо це контракт, транзакція чи проєкт, за допомогою яких особа інвестує гроші у спільне підприємство у відповідь на обіцянку отримання прибутку від діяльності засновника чи третьої сторони (Кричевська, 2017).

2.3. Службові токени (Utility Tokens) використовуються для доступу до послуг або функцій у межах певної платформи чи децентралізованого застосування, запропонованих емітентом. Наприклад, FileCoin, децентралізований додаток (DApp) для зберігання файлів, під час ICO пропонував монети FIL, які ви б використовували, щоб платити іншим користувачам за зберігання ваших файлів. У ході свого ICO Ethereum продавав етер, який є валютою, що використовується для оплати запуску смарт-контрактів і DApps. Слід зазначити, що регулятор може класифікувати службовий токен як цінний папір. Якщо ви купуєте службовий токен, щоб

заплатити авансом за використання послуги до того, як вона подорожує, службовий токен не є цінним папером, оскільки ви не очікуєте на прибуток, а просто хочете заощадити. Якщо ж ви хочете продати токени дорожче, коли послуга стане більш популярною, токен більше подібний до акції і з великою ймовірністю розглядатиметься регулятором як цінний папір (Mehta et al., 2021).

2.4. Токени управління – криптоактиви, які надають своїм власникам право голосу та впливу на прийняття рішень щодо розвитку проекту, на платформі якого ці токени були випущені (*Uniswap (UNI)*, *Maker (MKR)*).

2.5. Стейблкоїни. Вони призначені для зменшення волатильності, характерної для більшості криптовалют, і надання користувачам стабільного інструменту для зберігання та передачі цінності, сумісного з відповідною технологічною екосистемою. Стейблкоїни можуть бути забезпечені активами або алгоритмічні. Найчастіше забезпеченням стейблкоїна виступає одна з національних валют (долар США – *Tether (USDT)*, *USD Coin (USDC)*; євро: *Stasis Euro (EURS)*, *Tether Euro (EURT)*, *Circle Euro Coin (EUROC)*; британський фунт – *TrueGBP (TGBP)*; канадський долар – *QCAD*; сингапурський долар – *XSGD*; австралійський долар – *AUDT*; тайський бат – *THBEX*. Існує також стейблкоїн, прив'язаний до СПЗ (спеціальних прав запозичення МВФ) – *Saga (SGA)*. Стейблкоїни можуть бути забезпечені фізичними товарами. Фактично у цій групі існують лише стейблкоїни, забезпечені золотом (*PAX Gold (PAXG)*, *DigixDAO (DGX)*) з огляду на меншу стабільність та ліквідність інших фізичних активів. Проект випуску *Tiberius Coin (TCX)*, який мав бути забезпечений комбінацією металів – золота, платини, міді та інших, так і не було реалізовано, а сумнозвісний забезпечений нафтою стейблкоїн *Petro (PTR)*, випущений урядом Венесуели, є радше інструментом політичної маніпуляції, аніж справжнім стейблкоїном. Ще один вид стейблкоїнів – *забезпечені іншими криптоактивами* (як правило, з надлишковим забезпеченням) (*DAI*, про який йтиметься у другій статті цієї серії).

Алгоритмічні стейблкоїни підтримують стабільність ціни за допомогою алгоритмів, що змінюють їхню пропозицію залежно від ринкових умов (*TerraUSD (UST)* до її краху, *Ampleforth (AMPL)*).

Можливі і гібридні моделі стабілізації вартості стейблкоїнів. Наприклад, стейблкоїн *Frax* поєднує забезпечення активами і алгоритмічний механізм: якщо ціна падає нижче 1 дол. США, рівень забезпечення збільшується, і навпаки.

Попередником стейблкоїнів як віртуальних забезпечених активами грошей можна вважати створену у 1996 р. електронну платіжну систему E-gold компанії Gold & Silver Reserve Inc (Сент-Кітс і Невіс). Цифрові одиниці були забезпечені дорогоцінними металами, що зберігалися у банківському сейфі у Флориді, США. E-gold не вимагала підтвердження особи користувачів, і це робило її привабливою для злочинного світу; зрештою вебсайт було закрито через звинувачення у сприянні злочинності (Lewis, 2018). Втім, перші стейблкоїни, запущені на блокчейні, були саме алгоритмічні-

ми, тобто прагнули максимально дотримуватися логіки децентралізації (*BitUSD, NuBits*). Це були самореферентні системи з пар криптоактивів – стейблкоїна і криптоактиву з вільним курсоутворенням, у яких курс стейблкоїна вирівнювався за допомогою арбітражу. Усі вони зазнали краху, позаяк арбітраж припиняється в умовах паніки (у другій статті цієї серії ми розглянемо природу такого краху на прикладі екосистеми *Terra-Luna*).

2.6. Токенізовані активи реального світу – зокрема нерухомість, товари, акції, облигації. Це цифрові представлення активів, створені за допомогою технології розподіленого реєстру. Токенізація дозволяє перетворити права власності на актив на цифрові токени, які можуть бути передані, продані або використані як забезпечення на блокчейн-платформах.

2.7. Невзаємозамінні криптоактиви – криптоактиви, цінність яких походить від унікальних характеристик кожного криптоактиву та корисності, яку він надає власнику токена.

2.8. Заохочувальні токени – використовуються для стимулювання учасників до певної поведінки або внеску в мережу, наприклад, надання обчислювальних ресурсів, зберігання даних, створення контенту тощо. Так, на соціальній платформі Steem користувачі отримують токени STEEM за створення, коментування і вподобання контенту.

3. Соціально-економічні характеристики описують аспекти, що визначають особливості взаємодії користувачів з криптоактивом, а також його вартість, вплив на економіку і суспільство.

3.1. Стратегія пропозиції криптоактиву. Частина криптоактивів мають фіксовану пропозицію монет. *Визначений заздалегідь обсяг пропозиції може досягатися за програмно визначеним розкладом.* Ця стратегія пропозиції може бути вбудована безпосередньо в протокол консенсусу (як це відбувається у мережах *Bitcoin, Litecoin, Bitcoin Cash*), реалізована через один або кілька смарт-контрактів, які управляють екосистемою (*Freni et al., 2022*). У деяких випадках *визначений заздалегідь обсяг пропозиції криптоактиву досягається дискреційно за рішеннями розробників чи інших учасників екосистеми.* Хоча *XRP* має фіксовану загальну пропозицію, яка становить 100 млрд токенів, велика частина цих токенів зберігається в ескроу і поступово випускається на ринок. *BNB* був створений під час ICO, але не всі токени були випущені одночасно. З 200 млн *BNB* лише 100 млн було продано на ICO, а решта залишилася в резерві для команди *Binance* і стимулювання екосистеми. В мережі *EOS* більшість монет були продані або розподілені під час ICO, але частина була зарезервована для розробників та стимулювання екосистеми.

Інші криптоактиви мають *інфляційну пропозицію*: загальна кількість монет постійно зростає за певним алгоритмом (*Dogecoin, Shiba Inu*).

Елементом стратегії пропозиції криптоактиву може бути *опція спалювання частини монет з метою стабілізації його ціни* (*Binance Coin (BNB)*, де частина токенів регулярно знищується; *Ethereum*, де спалюється частина комісійних винагород за транзакції). Спалювання криптоактивів відбувається шляхом відправлення токенів на спеціальну "нульову адре-

су" або "burn address", з якої їх неможливо витратити. Такі адреси не мають приватного ключа, тому доступ до переказаних на них токенів стає неможливим.

Існують також криптоактиви з адаптивною пропозицією – механізм емісії динамічно змінюється залежно від певних параметрів мережі (наприклад ціни, кількості транзакцій). *Ampleforth (AMPL)* автоматично коригує пропозицію токенів пропорційно сумі у кожному гаманці, щоб за 1 AMPL можна було придбати той самий набір товарів, як у 2019 р. за 1 дол. США⁴.

Криптоактиви також можуть мати цілковито дискреційну пропозицію – токени карбуються і розподіляються без заздалегідь визначеного розкладу, відповідно до волі чи потреб емітента токенів або користувачів. Стейблкоїн *Tether (USDT)* прив'язаний до долара США, але його пропозиція є дискреційною, оскільки нові токени створюються і випускаються на ринок відповідно до попиту. *Tether Ltd.* може збільшити або зменшити кількість токенів на ринку на основі свого рішення та попиту користувачів. Хоча *DAI* є стейблкоїном з алгоритмічним контролем пропозиції, він також має елементи дискреційного управління. Токени *DAI* створюються шляхом застави інших криптоактивів, і кількість нових токенів залежить від рішень користувачів системи, які створюють нові застави або вилучають вже існуючі.

3.2. Рівень децентралізації – ступінь розподілу контролю та влади в мережі.

Повністю децентралізовані. Жоден учасник мережі не має більше влади, ніж інші, мережа працює на основі консенсусу, досягнутого всіма учасниками. Управління мережею *Bitcoin* здійснюється з допомогою майнерів, і зміни можуть бути внесені лише через суворий процес консенсусу. Втім, у багатьох таких мережах вагомий авторитет мають розробники програмного забезпечення, як-от *Bitcoin Core* для вузлів мережі біткоїна. Децентралізоване управління мережею криптоактиву може набувати форми *DAO (Decentralized Autonomous Organization)* – децентралізованої автономної організації з прозорим алгоритмом голосування і ухвалення рішень, часто вбудованим у смарт-контракти (*MakerDAO (MKR)*, *Uniswap (UNI)*, *Aave (AAVE)*, *Curve (CRV)*).

Децентралізовані з центральним управлінням оновленнями. Мережа децентралізована з точки зору роботи і транзакцій, але ключові оновлення або зміни в протоколі контролюються невеликою групою розробників або організацією. Хоча *Ethereum* є децентралізованою мережею, оновлення протоколу (наприклад переходи на нові версії) контролюються *Ethereum Foundation* та спільнотою розробників. Мережа *Cardano* має децентралізовану структуру з точки зору блокчейна та валідаторів, але розвиток і управління платформою здійснюються центральними організаціями (*IOHK*, *Emurgo*).

⁴ About the Ampleforth Protocol. *Ample*. URL: <https://docs.ampleforth.org/learn/about-the-ampleforth-protocol>

Квазіцентралізовані. Мережа має децентралізовану інфраструктуру, але управління основними аспектами мережі (наприклад вибір валідаторів, управління токенами) здійснюється через систему делегування або ж значна частина контролю зосереджена в руках компанії-розробника (*Tron, EOS, Ripple*).

Централізовані криптоактиви керуються компаніями або організаціями, які контролюють емісію, управління і резерви активів (*Tether (USDT), USD Coin (USDC), Binance Coin (BNB), FTX Token (FTT)* (до ліквідації біржі)).

3.3. Регульованість. Різні види криптоактивів, залежно від їхньої природи, ризиків, поширення, можуть ставати об'єктами більш чи менш жорсткого регулювання.

Висока регульованість передбачає дотримання криптоактивами відповідності вимогам національних або наднаціональних регуляторів чи нормативних актів. До цього виду можна віднести токени цінних паперів, а в ЄС також *токени електронних грошей* – тип криптоактивів, який має на меті підтримку стабільної вартості за допомогою прив'язки до вартості однієї офіційної валюти, та *токени, прив'язані до активів*, – тип криптоактиву, що не є токеном електронних грошей і який має на меті підтримку стабільної вартості за рахунок прив'язки до іншої вартості чи права або їхньої комбінації, в тому числі однієї чи кількох офіційних валют⁵.

Регульованість як системно важливих. Регламент ЄС "Про ринок криптоактивів" (MiCA – Markets in Crypto-Assets Regulation) визначає токени, прив'язані до активів, та токени електронних грошей як системно важливі, якщо вони відповідають щонайменше трьом критеріям, серед яких велика клієнтська база, висока ринкова капіталізація, велика кількість транзакцій, визнання емітента токена, прив'язаного до активу, постачальником базових послуг платформи, визначеного як гейткіпер відповідно до Регламенту (ЄС) 2022/1925 Європейського Парламенту та Ради (43) "Про конкурентні і справедливі ринки у цифровому секторі" та ін. До системно важливих токенів, прив'язаних до активів, та токенів електронних грошей висуваються суворіші вимоги, а їхнє регулювання в ЄС здійснюється не національними регуляторами, а наднаціональним банківським регулятором European Banking Authority.

Помірна регульованість проявляється в тому, що вони підпадають під деякі регуляторні вимоги, але не настільки жорсткі, як для стейблкоїнів або цінних паперів. Ці активи можуть мати часткові зобов'язання щодо прозорості, дотримання політик AML (Anti-Money Laundering), CFT (Combating the Financing of Terrorism) та KYC (Know Your Customer), або обмежені зобов'язання щодо реєстрації і звітності в деяких юрисдикціях. Такий підхід використовується до децентралізованих токенів, службових токенів, токенів управління, токенів проектів DeFi. Слід зазначити, що вимоги AML, CFT та KYC застосовуються до біткоіна, етеру та інших децентралізованих крип-

⁵ On markets in crypto-assets.

тоактивів, але не безпосередньо до самих активів або технології блокчейну, а до бірж та інших сервісів, що працюють з ними.

Низька або відсутня регульованість. Це можуть бути токени, які використовуються виключно в межах програм лояльності або як службові токени для доступу до певних послуг або продуктів у вузьких межах, а також NFT, які поки що не розглядаються як фінансові інструменти.

У другій статті цієї серії ми розглянемо "топографію криптопростору" – особливості та види проєктів, пов'язаних із 30 криптоактивами з найбільшим обсягом капіталізації, а також окреслимо тенденції взаємодії криптопростору з традиційним світом.

Висновки

Простір криптоактивів постав як втілення ідеології шифропанків, що протиставляє державному захисту прав власності і свобод забезпечення ефективною співпраці між людьми, зокрема засобу обігу і способу виконання контрактів, за допомогою анонімних, захищених криптографією децентралізованих взаємодій. Біткоїн став першим децентралізованим віртуальним платіжним засобом, що спирався на технології криптографії і розподіленого реєстру, Етеріум – першою блокчейн-платформою, середовищем, де можна створювати і запускати контракти, виконання яких не потребує участі посередників.

Розбудова простору криптоактивів відбувається в напрямках вирішення трилеми блокчейну про неможливість одночасного досягнення в блокчейні децентралізації, масштабованості і безпеки, з урахуванням цілей проєкту; забезпечення інтероперабельності децентралізованих мереж; створення нових форм співпраці з традиційними фінансовими посередниками та іншими інституціями традиційного світу (що вже йде в розріз з ідеологією шифропанків).

Уже відкритість коду біткоїна (його можна було копіювати, модифікувати й створювати нові блокчейни та нові криптовалюти) відкрила більш широкі можливості для створення фінансових активів, ніж у традиційному світі, а поява різноманітних інструментів, що пропонували простіші способи створення нових криптоактивів на чужих блокчейнах, передусім стандарту токенів ERC-20, перетворила простір криптоактивів на простір необмеженого створення фінансових активів. Це також дало імпульс зростанню вартості та волатильності криптоактивів і розвитку спекулятивної фінансової активності, пов'язаної з криптоактивами.

Характеристики криптоактивів можна об'єднати у три групи: технологічні, функціональні та соціально-економічні. Технологічні характеристики визначають, як саме конструкція криптоактиву вирішує проблеми безпеки, децентралізації, швидкості і вартості транзакцій, інтероперабельності з іншими віртуальними просторами і традиційним світом. Функціональні характеристики описують роль і призначення криптоактиву в екосистемі: для проведення платежів, участі в управлінні проєктом, отримання доступу до послуг або ресурсів і т. д. Соціально-економічні характеристики сто-

суються аспектів, що визначають особливості взаємодії користувачів з криптоактивом, а також його вартість, вплив на економіку і суспільство.

Література

1. Гриценко А. А. (2022). Економічні суперечності глобалізації і локалізації та їх сучасні прояви. *Економічна теорія*. № 4. С. 5–29. <https://doi.org/10.15407/etet2022.04.005>
2. Кричевська Т. (2017). Криптовалюти: фактори зростання та регуляторні реакції. *Ефективна економіка*. № 12. URL: <http://www.economy.nauka.com.ua/?op=1&z=5957>
3. Кричевська Т. О. (2018а). Перспективи криптовалют: про що говорить палітра альткоїнів. *Ефективна економіка*. № 12. URL: <http://www.economy.nauka.com.ua/?op=1&z=6787>. <https://doi.org/10.15407/etet2022.04.00510.32702/2307-2105-2018.12.110>
4. Кричевська Т. О. (2018b). Технологія розподіленого реєстру: теоретико-інституційні засади, потенціал, фактичні досягнення та соціально-економічне значення. *Ефективна економіка*. № 11. <https://doi.org/10.32702/2307-2105-2018.11.84>
5. Кричевська Т.О. (2024). Криптовалюти: легалізація та соціально-економічні трансформації. *Економічні перспективи підприємництва: виклики воєнного часу та повоєнної відбудови* [Електронне видання]: збірник матеріалів VII Міжнародної науково-практичної конференції (м. Ірпінь, 31 травня 2024 р.) Ірпінь: Державний податковий університет. С. 42–46. URL: https://dpu.edu.ua/images/2024/Photo_dlya_novyn_2024/Kafedra%20ekonomiki%20pidpriemnictva%20ta%20biznes-administruvanna/ZBIRNIK_Konferencia_Ekonomichni_perspektivi_pidpriemnictva_31.05.2024_.pdf
6. Міщенко В.І., Науменкова С.В., Міщенко С.В. (2022). Теоретичні засади та практичні аспекти впровадження і використання цифрових грошей. *Економічна теорія*. № 2. С. 44–66. <https://doi.org/https://doi.org/10.15407/etet2022.02.044>
7. Bech M., Garratt R. (2017). Central bank cryptocurrencies. *BIS Quarterly Review*. September, 55–70. URL: https://www.bis.org/publ/qtrpdf/r_qt1709.pdf
8. Benos E. et al. (2017). The economics of distributed ledger technology for securities settlement. *Bank of England Staff Working Paper*. August No. 670. URL: <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf>
9. Bjelic M. et al. (2023). POL: One token for all Polygon chains. *Polygon*. URL: <https://polygon.technology/papers/pol-whitepaper>
10. Bouri E. et al. (2017). On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? *Finance Research Letters*, 20, 192–198. <https://doi.org/10.1016/j.frl.2016.09.025>
11. Chipolina S. et al. (December 5, 2023). Binance's \$4.3bn fine was set high as a warning, says US regulator. *Financial Times*. URL: <https://www.ft.com/content/81bdaf30-3f61-4ff4-b579-805a4af8f8e1>
12. Coelho R. et al. (2021). Supervising cryptoassets for anti-money laundering. *FSI Insights on policy implementation*. April. № 31. URL: <https://www.bis.org/fsi/publ/insights31.htm>
13. Corbe S. et al. (2018). Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters*. Vol. 165, issue C. 28–34. <https://doi.org/10.1016/j.econlet.2018.01.004>
14. Cryptoslav I. (2022). What Is Polygon? The Ultimate Guide to the Polygon Ecosystem. *Coin Market Cap*. URL: <https://coinmarketcap.com/academy/article/what-is-polygon-the-ultimate-guide-to-the-polygon-ecosystem>
15. Dai W. (November, 1998). b-money. *Satoshi Nakamoto Institute*. URL: <https://nakamotoinstitute.org/library/b-money/>
16. Dash A. (November 14, 2021). On "inventing NFTs" and how we don't have any good way to talk about tech. URL: <https://www.anildash.com/2021/11/14/i-didnt-invent-nfts-but-we-dont-really-have-any-other-way-to-talk-about-tech/>

17. De Filippi P., Wright A. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press. <https://doi.org/10.4159/9780674985933>
18. Delisle B. (2018). SATIS Group Report: "78% of ICOs Are Scams". *CryptoSlate*. URL: <https://cryptoslate.com/satis-group-report-78-of-icos-are-scams>
19. Diffie W., Hellman M. (November, 1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*. Vol. It-22, issue 6. URL: <https://www.ee.stanford.edu/~hellman/publications/24.pdf>; <https://doi.org/10.1109/TIT.1976.1055638>
20. Dutta B. (April 8, 2022). 5 Types of Distributed Ledger Technologies (DLT). *Analyticssteps*. URL: <https://www.analyticssteps.com/blogs/5-types-distributed-ledger-technologies-dlt>
21. Dwork C., Naor M. (1993). Pricing via Processing or Combatting Junk Mail. Brickell, E.F. (eds) *Advances in Cryptology – CRYPTO' 92*. Lecture Notes in Computer Science, Vol 740. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48071-4_10
22. Ellis S. et al. (4 September, 2017). ChainLink: A Decentralized Oracle Network. V1.0. URL: <https://research.chain.link/whitepaper-v1.pdf>
23. Euler T. (January 18, 2018). The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens. *Untitled INC*. URL: <https://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/>
24. Final Report with Policy Recommendations for Decentralized Finance (DeFi). (December, 2023). IOSCO. URL: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf>
25. Freni P. et al. (March, 2022). Tokenomics and blockchain tokens: A design-oriented morphological framework. *Blockchain: Research and Applications*. Volume 3, issue 1. URL: <https://www.sciencedirect.com/science/article/pii/S2096720922000094>; <https://doi.org/10.1016/j.bcr.2022.100069>
26. Garrido J. M. (2023). Digital Tokens: A Legal Perspective. *IMF Working Paper*. March, WP/23/151. URL: <https://www.imf.org/en/Publications/WP/Issues/2023/07/28/Digital-Tokens-A-Legal-Perspective-537041>; <https://doi.org/10.5089/9798400250149.001>
27. Goldman K., Kumar A. (2021). A Taxonomy of Digital Assets. Milken Institute. URL: <https://milkeninstitute.org/sites/default/files/2021-10/A%20Taxonomy%20of%20Digital%20Assets.pdf>
28. Griffin J. M. Shams A. (October 28, 2019). Is Bitcoin Really Un-Tethered? *SSRN*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066; <https://dx.doi.org/10.2139/ssrn.3195066>
29. Guesmi K. et al. (2019). Portfolio diversification with virtual currency: Evidence from bitcoin. *International Review of Financial Analysis*, 63, 431–437. <https://doi.org/10.1016/j.irfa.2018.03.004>;
30. Kelly J., Thornhill J. (2022). A sceptic's guide to crypto: the "smart" money. How Silicon Valley bought into Web3. Tech Tonic. Transcript. *Financial Times*. August 23. URL: <https://www.ft.com/content/e095c79b-e66c-4482-9b52-87e6c9b936b3>
31. Kruppa M. et al. (2022). The great NFT sell-off: has the digital collectibles craze hit its peak? *Financial Times*. March 11. URL: <https://www.ft.com/content/46349496-790a-4223-8c65-d6a0bde897bc>
32. Levy S. (2002). *Crypto: How the code rebels beat the government – saving privacy in the digital age*. London: Penguin Books.
33. Lewis A. (2018) *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them*. Coral Gables: Mango Publishing.
34. Mehta N. et al. (2021). *Bubble or Revolution? The Present and Future of Blockchain and Cryptocurrencies*. Paravane Ventures. 2nd Edition, 2nd Revision
35. *Metaverse and Money: Decrypting the Future*. (2022). Citi GPS: Global Perspectives & Solutions. March Citigroup. URL: https://www.citigroup.com/global/insights/metaverse-and-money_20220330;
36. Murphy H., Oliver J. (2021, December 31,). How NFTs became a \$40bn market in 2021. *Financial Times*. URL: <https://www.ft.com/content/e95f5ac2-0476-41f4-abd4-8a99faa7737d>
37. My first impressions of web3. (January 7, 2022). URL: <https://moxie.org/2022/01/07/web3-first-impressions.html>

38. Nguyen Kh. Q. (May, 2022). The correlation between the stock market and Bitcoin during COVID-19 and other uncertainty periods. *Finance Research Letters*. Vol. 46, part A, 102284. URL: <https://www.sciencedirect.com/science/article/pii/S1544612321003238>
39. Oliver J. Hype Machine: How Greed, Fraud and Free Money Crashed Crypto. London: Heligo Books, 2024.
40. Sharding FAQ. (December 31, 2017). URL: https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html
41. Szabo N. (1996). Smart Contracts: Building Blocks for Digital Markets. *True value metrics for a smart society*. URL: <https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf>
42. The 2024 Crypto Crime Report. (February, 2024). Chainalysis. URL: <https://go.chainalysis.com/crypto-crime-2024.html>
43. The market for non-fungible tokens is evolving. *The economist*. (October 29, 2021). URL: <https://www.economist.com/finance-and-economics/2021/10/29/the-market-for-non-fungible-tokens-is-evolving>
44. Virtual Currencies and Beyond: Initial Considerations. (2016). IMF Staff Discussion Note. *IMF*. URL: <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>;
45. Waters R. Web3's messy vision of a tech future. (December 23, 2021). *Financial Times*. <https://www.ft.com/content/f33aa1fe-7fde-4bf9-b89d-22c6455cf7af>
46. Werbach K., Cornell N. (2017). Contracts Ex Machina. *Duke Law Journal*. Vol. 67, issue 2, 313–382. URL: <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dlj>

Надходження до редакції 1 листопада 2024 року

Прорецензовано 8 листопада 2024 року

Підписано до друку 6 грудня 2024 року

References

- Grytsenko, A. A. (2022). Economic contradictions of globalization and localization and their modern manifestations. *Ekon. teor. – Economic theory*, 4, 5-29. Retrieved from <https://doi.org/10.15407/etet2022.04.005> [in Ukrainian].
- Krychevska, T. O. (2017). Cryptocurrencies: growth factors and regulatory reactions. *Efektivna ekonomika – Efficient economy*, 12. Retrieved from <http://www.economy.nayka.com.ua/?op=1&z=5957> [in Ukrainian].
- Krychevska, T. O. (2018a). Prospects of cryptocurrencies: what does altcoins palette tell us. *Efektivna ekonomika – Efficient economy*, 12. Retrieved from: <http://www.economy.nayka.com.ua/?op=1&z=6787>; <https://doi.org/10.32702/2307-2105-2018.12.110> [in Ukrainian].
- Krychevska, T. O. (2018b). Distributed ledger technology: theoretical and institutional foundations, potential, actual achievements, and socio-economic role. *Efektivna ekonomika – Efficient economy*, 11. Retrieved from <http://www.economy.nayka.com.ua/?op=1&z=6687>; <https://doi.org/10.32702/2307-2105-2018.11.84> [in Ukrainian].
- Krychevska, T. O. (2024). Cryptocurrencies: Legalization and Socio-Economic Transformations. *Economic Prospects of Entrepreneurship: Challenges of Wartime and Post-War Reconstruction* [Electronic Edition]: Collection of materials of the VII International Scientific and Practical Conference (Irpın, May 31, 2024). Irpın: State Tax University: 42–46. Retrieved from https://dpu.edu.ua/images/2024/Photo_dlya_novyn_2024/Kafedra%20ekonomiki%20pidpriemnictva%20ta%20biznes-administrivanna/ZBIRNIK_Konferencia_Ekonomichni_perspektivi_pidpriemnictva_31.05.2024_.pdf [in Ukrainian].
- Mishchenko, V. et al. (2022). Theoretical fundamentals and practical aspects of the implementation and use of digital money. *Ekon. teor. – Economic theory*, 2: 44-66. <https://doi.org/10.15407/etet2022.02.044> [in Ukrainian].
- Bech, M., Garratt, R. (September, 2017). Central bank cryptocurrencies. *BIS Quarterly Review*, 55-70. Retrieved from https://www.bis.org/publ/qtrpdf/r_qt1709.pdf

8. Benos, E. et al. (2017). The economics of distributed ledger technology for securities settlement. *Bank of England Staff Working Paper*, August. Retrieved from <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2017/the-economics-of-distributed-ledger-technology-for-securities-settlement.pdf>
9. Bjelic, M. et al. (2023). POL: One token for all Polygon chains. *Polygon*. Retrieved from <https://polygon.technology/papers/pol-whitepaper>
10. Bouri, E. et al. (2017). On the hedge and safe haven properties of Bitcoin: Is it really more than a diversifier? *Finance Research Letters*, 20, 192-198. <https://doi.org/10.1016/j.frl.2016.09.025>
11. Chipolina, S. et al. (December 5, 2023). Binance's \$4.3bn fine was set high as a warning, says US regulator. *Financial Times*. Retrieved from <https://www.ft.com/content/81bdaf30-3f61-4ff4-b579-805a4af8f8e1>
12. Coelho, R. et al. (2021). Supervising cryptoassets for anti-money laundering. *FSI Insights on policy implementation*, April, 31. Retrieved from <https://www.bis.org/fsi/publ/insights31.htm>
13. Corbe, S. et al. (2018). Exploring the dynamic relationships between cryptocurrencies and other financial assets. *Economics Letters*, 165(C), 28-34. <https://doi.org/10.1016/j.econlet.2018.01.004>
14. Cryptoslav, I. (2022). What Is Polygon? The Ultimate Guide to the Polygon Ecosystem. *Coin Market Cap*. Retrieved from <https://coinmarketcap.com/academy/article/what-is-polygon-the-ultimate-guide-to-the-polygon-ecosystem>
15. Dai, W. (November, 1998). b-money. *Satoshi Nakamoto Institute*. Retrieved from <https://nakamotoinstitute.org/library/b-money/>
16. Dash, A. (November 14, 2021). On "inventing NFTs" and how we don't have any good way to talk about tech. Retrieved from <https://www.anildash.com/2021/11/14/i-didnt-invent-nfts-but-we-dont-really-have-any-other-way-to-talk-about-tech/>
17. De Filippi, P., Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press. <https://doi.org/10.4159/9780674985933>
18. Delisle, B. (2018). SATIS Group Report: "78% of ICOs Are Scams". *CryptoSlate*. Retrieved from <https://cryptoslate.com/satis-group-report-78-of-icos-are-scams>
19. Diffie, W., Hellman, M. (November, 1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, It-22(6). Retrieved from <https://www.ee.stanford.edu/~hellman/publications/24.pdf>; <https://doi.org/10.1109/TIT.1976.1055638>
20. Dutta, B. (April 8, 2022). 5 Types of Distributed Ledger Technologies (DLT). *AnalyticsSteps*, Retrieved from <https://www.analyticssteps.com/blogs/5-types-distributed-ledger-technologies-dlt>
21. Dwork, C., Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. In *Brickell, E.F. (eds.) Advances in Cryptology – CRYPTO'92. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer. https://doi.org/10.1007/3-540-48071-4_10
22. Ellis, S. et al. (September 4, 2017). ChainLink: A Decentralized Oracle Network. V1.0. Retrieved from <https://research.chain.link/whitepaper-v1.pdf>
23. Euler, T. (2018). The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens, January 18. *Untitled INC*. Retrieved from <https://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/>
24. Final Report with Policy Recommendations for Decentralized Finance (DeFi). (2023). *IOSCO*, December. Retrieved from <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf>
25. Freni, P. et al. (March, 2022). Tokenomics and blockchain tokens: A design-oriented morphological framework. *Blockchain: Research and Applications*, 3(1). Retrieved from <https://www.sciencedirect.com/science/article/pii/S2096720922000094>; <https://doi.org/10.1016/j.bcra.2022.100069>
26. Garrido, J. M. Digital Tokens: A Legal Perspective. (2023). *IMF Working Paper*, March, WP 23(151). Retrieved from <https://www.imf.org/en/Publications/WP/Issues/2023/07/28/Digital-Tokens-A-Legal-Perspective-537041>; <https://doi.org/10.5089/9798400250149.001>
27. Goldman, K., Kumar, A. (2021). A Taxonomy of Digital Assets. Milken Institute. Retrieved from <https://milkeninstitute.org/sites/default/files/2021-10/A%20Taxonomy%20of%20Digital%20Assets.pdf>

28. Griffin, J. M. Shams, A. (October 28, 2019). Is Bitcoin Really Un-Tethered? *SSRN*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066; <https://dx.doi.org/10.2139/ssrn.3195066>
29. Guesmi, K. et al. (2019). Portfolio diversification with virtual currency: Evidence from bitcoin. *International Review of Financial Analysis*, 63, 431-437. Retrieved from <https://doi.org/10.1016/j.irfa.2018.03.004>
30. Kelly, J., Thornhill, J. (August 23, 2022). A sceptic's guide to crypto: the "smart" money. How Silicon Valley bought into Web3. Tech Tonic. Transcript. *Financial Times*. Retrieved from <https://www.ft.com/content/e095c79b-e66c-4482-9b52-87e6c9b936b3>
31. Kruppa, M. et al. (2022). The great NFT sell-off: has the digital collectibles craze hit its peak? *Financial Times*, March 11. Retrieved from <https://www.ft.com/content/46349496-790a-4223-8c65-d6a0bde897bc>
32. Levy, S. (2002). *Crypto: How the code rebels beat the government – saving privacy in the digital age*. London: Penguin Books.
33. Lewis, A. (2018). *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them*. Coral Gables: Mango Publishing.
34. Mehta, N. et al. (2021). *Bubble or Revolution? The Present and Future of Blockchain and Cryptocurrencies*. Paravane Ventures. 2nd Edition, 2nd Revision
35. *Metaverse and Money: Decrypting the Future*. (March, 2022). Citi GPS: Global Perspectives & Solutions. *Citigroup*. Retrieved from https://www.citigroup.com/global/insights/metaverse-and-money_20220330;
36. Murphy, H., Oliver, J. (2021, December 31). How NFTs became a \$40bn market in 2021. *Financial Times*. Retrieved from <https://www.ft.com/content/e95f5ac2-0476-41f4-abd4-8a99faa7737d>
37. My first impressions of web3. (January 7, 2022). Retrieved from <https://moxie.org/2022/01/07/web3-first-impressions.html>;
38. Nguyen, Kh. Q. (2022). The correlation between the stock market and Bitcoin during COVID-19 and other uncertainty periods. *Finance Research Letters*, 46(A). Retrieved from <https://www.sciencedirect.com/science/article/pii/S1544612321003238>; <https://doi.org/10.1016/j.frl.2021.102284>
39. Oliver, J. (2024). *Hype Machine: How Greed, Fraud and Free Money Crashed Crypto*. London: Heligo Books,
40. Sharding FAQ. (December 31, 2017). Retrieved from https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html
41. Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. *True value metrics for a smart society*. Retrieved from <https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf>
42. The 2024 Crypto Crime Report. (2024). *Chainalysis*, February. Retrieved from <https://go.chainalysis.com/crypto-crime-2024.html>
43. The market for non-fungible tokens is evolving. *The economist*. (October 29, 2021). Retrieved from <https://www.economist.com/finance-and-economics/2021/10/29/the-market-for-non-fungible-tokens-is-evolving>
44. *Virtual Currencies and Beyond: Initial Considerations*. (2016). *IMF Staff Discussion Note*. IMF. Retrieved from <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>;
45. Waters, R. (December 23, 2021). Web3's messy vision of a tech future. *Financial Times*. Retrieved from <https://www.ft.com/content/f33aa1fe-7fde-4bf9-b89d-22c6455cf7af>
46. Werbach K., Cornell N. (2017). *Contracts Ex Machina*. *Duke Law Journal*, 67(2), 313-382. Retrieve from <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3913&context=dj>

Received November 1, 2024

Reviewed November 28, 2024

Signed to print December 6, 2024.