

ТЕХНІКО-ПРАВОВЕ РІЗНОМАНІТТЯ В ПРОЯВАХ ХАРАКТЕРИСТИК ВІДПОВІДНОСТІ КРИПТОВАЛЮТИ: МІЖДИСЦИПЛІНАРНЕ ДОСЛІДЖЕННЯ

TECHNICAL AND LEGAL DIVERSITY IN THE MANIFESTATIONS OF CRYPTOCURRENCY COMPLIANCE CHARACTERISTICS: AN INTERDISCIPLINARY STUDY

Василенко М.Д., д.фіз.-мат.н., д.ю.н., професор,
професор кафедри кібербезпеки, професор кафедри господарського права і процесу
Національний університет «Одеська юридична академія»

Слатвінська В.М., лауреат щорічного Всеукраїнського конкурсу «Молодий вчений року» 2022,
експерт комп'ютерно-технічних експертиз,
асистент кафедри кібербезпеки
Національний університет «Одеська юридична академія»

У статті з'ясовано встановлення різноманіття та визначення характеристик відповідності криптовалюти та їх розуміння. Техніко-правове різноманіття відповідності криптовалюти охоплює як технічні характеристики, так і правовий статус цифрових активів – криптовалют. Техніко-правове різноманіття криптовалюти включає в себе різні технології, що використовуються для створення та функціонування цифрових валют, а також правовий статус криптовалют у різних юрисдикціях. Відповідність криптовалюти може бути розглянута з різних точок зору, включаючи технологічну, правову, фінансову та соціальну відповідність.

Зосереджено увагу на понятті «блокчейн», протоколах безпеки криптовалют, децентралізованих додатках, процедурі транзакції в Ethereum, майнінгу, алгоритмі доказу роботи стосовно до Ethereum.

З'ясовано, що криптовалюти базуються на криптографічних принципах, таких як притаманні блокчейну, та існує розподілена система реєстрації (DLT).

Авторами акцентовано увагу на описі процедури генерації адреси в Ethereum за допомогою криптографічного шифрування з урахуванням алгоритму еліптичної кривої *secp256k1* оскільки він є необхідним для розуміння криптовалют в цілому і без нього неможливо обговорювати криптовалюти, в тому числі й в юридичній літературі.

Доведено, що усі децентралізовані додатки, які використовують доказ виконання роботи не використовують абсолютно однаковий набір алгоритмів. Вони можуть відрізнятися в деталях щодо того, яке завдання має вирішити майнер, наскільки складним має бути завдання, скільки часу займає рішення і т. п. Авторами розглянуто алгоритм доказу роботи стосовно до Ethereum.

Характеристики відповідності криптовалюти можуть змінюватись в залежності від кожної конкретної криптовалюти та контексту використання. Важливо враховувати як технічні, так і правові аспекти, а також вплив на фінансову та соціальну сфери для повного розуміння відповідності криптовалюти.

Ключові слова: блокчейн-технологія, криптовалюта, віртуальні блага, біткоїн, ефіріум, ринок, цифрові гроші, віртуальні валюти, господарське право.

The article clarifies the establishment of the diversity and definition of the characteristics of cryptocurrency compliance and their understanding. The technical and legal diversity of cryptocurrency compliance covers both the technical characteristics and the legal status of digital assets – cryptocurrencies. The technical and legal diversity of cryptocurrencies includes various technologies used to create and operate digital currencies, as well as the legal status of cryptocurrencies in different jurisdictions. Cryptocurrency compliance can be viewed from a variety of perspectives, including technological, legal, financial, and social compliance.

The course focuses on the concept of blockchain, cryptocurrency security protocols, decentralized applications, Ethereum transaction procedures, mining, algorithm for proving the robot's work in accordance with Ethereum.

It is found that cryptocurrencies are based on cryptographic principles, such as those inherent in the blockchain, and there is a distributed ledger system (DLT).

The authors focus on the description of the procedure for generating an address in Ethereum using cryptographic encryption with the *secp256k1* elliptic curve algorithm, since it is essential for understanding cryptocurrencies in general and without it is impossible to discuss cryptocurrencies, including in the legal literature.

It has been proven that all decentralized applications that use proof of work do not use the same set of algorithms. They may differ in detail regarding what task a miner must solve, how complex the task should be, how long it takes to solve, etc. The authors consider the proof-of-work algorithm in relation to Ethereum.

The characteristics of cryptocurrency compliance may vary depending on each specific cryptocurrency and the context of use. It is important to consider both technical and legal aspects, as well as financial and social impacts to fully understand cryptocurrency compliance.

Key words: blockchain technology, cryptocurrency, virtual goods, bitcoin, ethereum, market, digital money, virtual currencies, commercial law.

Постановка проблеми. Криптовалюта визначається як електронно-цифрова грошова одиниця, що впроваджується в обіг протягом останніх десятиліть без контролю центрального банку конкретних держав. На відміну від електронної валюти, криптовалюта, що представлена біткоїном, ефіріумом та ін. – це віртуальні валюти, які не мають фізичного вираження. Одиницею подібної валюти традиційно є так званий коїн (з англійської – монети; натомість жодних монет у класичному сенсі не існує). Коїн є зашифрованою інформацією, яку неможливо скопіювати. Сьогодні у світі налічується більше восьми тисяч криптовалют, найпопулярнішими з яких частіше називають Bitcoin та Ethereum. Можна погодитися з тим, що досі криптовалютою вважають «цифровий актив, призначений

для роботи як засіб обміну з використанням криптографії для забезпечення транзакцій та контролю за створенням додаткових одиниць валюти» [1]. Однак, як вже було відзначено, існує безліч різновидів криптовалюти (bitcoin, ethereum, ripple, litcoin тощо). При цьому Біткоїн поки що займає провідну позицію. Деякі з криптовалют стали успішними, але більшість залишилися непопулярними і не знали успіху через брак інтересу. Було кілька прецедентів шахрайства, які незабаром зникли. Альтернативи біткоїну можна поділити на два типи, ґрунтуючись на меті їх розробки. Перший – полягає у побудові децентралізованої платформи блокчейну, їх називають альтернативними ланцюгами; коли метою стає створення нової віртуальної валюти, а сам проект проект називається Altcoin.

Альтернативні проекти базуються на альтернативних блокчейнах, основною метою яких є створення нової віртуальної валюти (койну). В цьому випадку створюють альтернативні протоколи, що надбудовані над біткойном для надання різних сервісів. Вони входять такі концепції, як Namecoin, основний метою якого є надання послуг децентралізованого неймінгу та ідентифікації замість валюти. Наприкінці 2018 року на ринку з'явилися сотні альтернативних валют, що мають грошову вартість, такі як Namecoin, Zcash, Primecoin та інші. Так, в останні роки Zcash стала більш успішною валютою, хоча була представлена ще з 2016 року. З іншого боку, Primecoin не набув особливої популярності, проте досі використовується. Багато інших альтернативних проектів представляють собою похідні від вихідного коду Bitcoin, незважаючи на те, що деякі з них були написані з нуля. Деякі альтернативи покликані обійти обмеження Bitcoin, такі як приватність. Інші надають різні типи майнінгу, зміни у часі блоків та інші типи розподілу. Так сталося, що автори цієї роботи є фахівцями юристами-господарниками, які ще професійно займаються інформаційними технологіями.

Аналіз останніх досліджень і публікацій. Проблема криптовалюти пов'язана з розумінням та регулюванням технологій блокчейну, на якій заснована технологічна база криптовалют. Авторами [2] показано, що при технологіях блокчейн використання криптографічних систем дозволяє створити нові можливості конфіденційності й швидкості обміну інформацією та керування, виявленими в проявах технологій блокчейн. Важливим компонентом такої системи стає «ключ», який представляє першу ланку в ланцюзі блокчейну. Він може зберігатися поза системою і використовуватися для різних перевірок в діяльності організації. Наголошено на нові можливості конфіденційності й швидкості обміну інформацією та керування може зберігатися поза системою і використовуватися для різних перевірок. З наукової точки зору використання в майбутньому технологій блокчейн веде до потреби в проведенні міждисциплінарних досліджень та їх застосування для різних додатків для визначення стратегій і соціальних наслідків такого застосування, цілісністю і повнотою використаних даних [2]. Автори [3] влучно зауважують, що блокчейн дозволяє позбавитися довірчих посередників і повністю децентралізувати транзакції довільних типів між будь-якими учасниками конкретної системи взаємовідносин в глобальному масштабі (вчені-господарники на це раніше не вказували). В роботі цих же авторів вказано на деяких авторів-юристів, які якимсь чином торкалися проблем блокчейну і криптовалют. Зрозуміло, що проблема криптовалюти багатогранна та міжгалузева. Автори [3] вважають, що існують різні обгрунтовані погляди на визначення криптовалюти як грошових засобів, нематеріальних активів, товару тощо. Відзначається багато переваг у використанні криптовалют в порівнянні з традиційними фінансовими інструментами. Разом з тим вказується, що криптовалюти незабезпечені активами та їх обіг мало контролюється державними інституціями, що несе чисельні фінансові, соціальні і навіть безпекові ризики. В той же час науковці-юристи й економісти продовжують дискутувати щодо розуміння природи криптовалюти, а існуюча законодавча та судова невизначеність в питанні обігу криптовалют додає хаотичності та бесистемності суспільним відносинам, пов'язаним з їх використанням (див. [3]).

Законодавство України намагається активно розвиватися у цьому напрямі, однак потребує реалізації та компетентних висновків. Сьогодні воно не забороняє, але і не визначає її реально діючий статус. Протягом останніх років було запропоновано низку законопроектів з приводу обігу криптовалют, однак на теперішній час, попри прийняття Закону України «Про віртуальні активи» [4] (набере чинності тільки після внесення відповідних змін

до Податкового кодексу України), «криптовалюта» значною мірою залишається поза правовим полем. Відзначимо, що автори [3] влучно зауважили той факт, коли йдеться про використання криптовалюти у договірних стосунках, це означає, що зазвичай її конвертують у національну чи світову резервну валюту для подальшого проведення розрахунків або уникають її деталізації при визначенні предмету договору. Безперечно, це створює певні колізії та підриває довіру до криптовалюти в цілому.

Метою статті є встановлення різноманіття та визначення характеристик відповідності криптовалюти та їх розуміння.

Виклад основного матеріалу. Для розуміння характеристик відповідності криптовалюти потрібно розуміння блокчейну в цьому питанні. В цьому випадку блокчейн представляє собою особливу структуру даних, що використовується для створення децентралізованого реєстру. Децентралізований розподілений реєстр визначається у способі реалізації списку транзакцій, що зберігаються в децентралізованій формі без прив'язки до географічної чи іншої приналежності вузлів мережі. Сам же блокчейн складається з блоків, особливим чином з'єднаних у ланцюжок [5, с. 291]. Блок містить набір транзакцій, хеш (хешування – це перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини); їх також називають хеш-функціями, або функціями згортання, а їхні результати називають хешем, хеш-кодом, хеш-сумою, або дайджестом повідомлення попереднього блоку, мітку часу (час створення блоку), суму відрахування майнера (діяльності створення нових структур, зазвичай йдеться про нові блоки в блокчейні) для забезпечення функціонування криптовалютних платформ. Оскільки кожен блок містить хеш попереднього блоку, вони теж пов'язані в ланцюжок. Кожен вузол мережі зберігає повну копію блокчейну.

Для підтримки безпеки блокчейна застосовують протоколи з доказом виконання роботи (proof-of-work, PoW), з доказом володіння часткою (proof-of-stake, PoS) та деякі інші. Додавання блоку відбувається по-різному – залежно від протоколу. У випадку протоколу proof-of-work блок створюється за допомогою процедури, яка називається майнінгом та забезпечує безпеку додавання блоку. Майнер повинен вирішити складне математичне завдання та витратити дорогі обчислювальні ресурси.

У мережі Bitcoin блокчейн зберігає транзакції Bitcoin. Біткойни (монети) вводяться в обіг шляхом виплати винагороди майнерам, які успішно створили нові блоки. Основною перевагою блокчейну є автоматизація контролю над безпекою транзакцій. Блокчейн запобігає шахрайству та зловживанням і може вирішити безліч інших проблем, залежно від способу реалізації та використання. Майже всі інтернет-програми, з якими ми мали справу, є централізованими, тобто сервери такої програми належать певній компанії чи особі. Протягом тривалого часу розробники створювали централізовані програми, а користувачі їх застосовували. Але такий підхід має проблеми, які заважають створювати певні типи додатків. Централізовані програми менш прозорі, мають конкретну точку відмови, що неспроможні протистояти мережевої цензурі тощо. На тлі цих проблем виникла нова технологія розробки інтернет-додатків, які називаються децентралізованими додатками. Вони і використовуються при створенні криптовалют. Децентралізовані додатки (ДД) представляють собою особливий різновид інтернет-додатків, що базуються на одноранговій мережі (peer-to-peer network) і мають відкритий вихідний код. Жоден вузол мережі немає повного контролю над ДД. Структура та спосіб зберігання даних ДД залежить від його функціонального призначення. Наприклад, Bitcoin використовує структуру даних як блокчейна. Злом однорангової мережі може стати будь-який комп'ютер, під-

ключений до Інтернету. Це створює серйозну проблему, пов'язану з необхідністю виявляти та блокувати вузли, що вносять помилкові зміни в дані та розповсюджують недостовірну інформацію іншим вузлам. Отже, ми повинні дійти згоди між вузлами щодо того, чи є достовірними дані, опубліковані певним вузлом. У структурі ДД немає головного сервера, який координує вузли та приймає рішення щодо достовірності даних. Для вирішення цієї вельми складної задачі призначені спеціальні протоколи консенсусу. Протоколи консенсусу розробляють під конкретну структуру даних ДД. Наприклад, Bitcoin для досягнення консенсусу використовує протокол доказу роботи (proof-of-work protocol, PoW). Кожний ДД має клієнтську частину (програма-клієнт), з якою працює користувач. Щоб отримати доступ до ДД, ми маємо стати вузлом однорангової мережі та запустити на своєму комп'ютері спеціальний сервер вузла, а потім підключити до цього сервера клієнт. Вузли програми надають лише API (Application Programming Interface, інтерфейс прикладного програмування) та дозволяють спільноті розробників створювати різні клієнтські програми. Деякі розробники ДД надають користувачам офіційну версію клієнта.

Клієнти повинні мати відкритий вихідний код і бути доступними для завантаження без обмежень. Інакше вся ідея децентралізації втрачає сенс.

Однак клієнт-серверна архітектура може виявитися важкою для встановлення, особливо якщо користувач не має навичок розробника. Тому зазвичай клієнт та/або сервер просто запускаються як служби.

Технологія блокчейн має великий потенціал у розвитку міжнародної торгівлі. До 2030 року за допомогою цих технологій міжнародна торгівля може збільшитися на 866 мільярдів доларів [6, с. 111]. Це станеться за рахунок:

- вдосконалення міжнародних торговельних розрахунків, які проводять миттєві платежі за відвантажені товари або послуги з гарантованою безпекою платежів, що призведе до збільшення товарообігу;
- застосування смарт-контрактів, які покращують контроль та якість послуг, а також прискорюють експортно-імпорتنі операції
- покращення логістичного ланцюга за рахунок зменшення паперового документообігу та втрат від нелегальних або сірих поставок;
- зменшення вартості посередницьких послуг за рахунок скорочення банківських послуг на 11%;
- розвиток торгівлі інтелектуальними товарами, які будуть захищені від піратського використання і тим самим збільшать рівень продажів;
- організація державних закупівель, завдяки яким можна буде вдасться вивести 20% всіх закупівель з-під корупційних схем [6, с. 111].

Техніко-правове різноманіття відноситься до різних аспектів технології та правового регулювання, які впливають на криптовалюти. Давайте розглянемо деякі з них:

1. Технічні характеристики криптовалюти: Криптовалюти базуються на блокчейн-технології, яка дозволяє створювати безпечні, децентралізовані і недвоїсті записи транзакцій. Кожна криптовалюта має свій власний протокол і алгоритм, наприклад, Bitcoin використовує SHA-256, Ethereum – Ethash, і так далі.

2. Децентралізація: криптовалюти, такі як Bitcoin та Ethereum, працюють на принципі децентралізації, що означає відсутність центральної влади або установи, яка контролює їх. Це робить їх відмінними від традиційних фіатних валют, які контролюються центральними банками.

3. Анонімність і приватність: Деякі криптовалюти, наприклад, Monero та Zcash, надають більш високий рівень анонімності та приватності у порівнянні з Bitcoin. Вони використовують різні технології, щоб забезпечити невідслідковуваність транзакцій та балансів.

4. Складність майнінгу: Майнінг – це процес, за допомогою якого нові токени криптовалюти створюються і нові транзакції перевіряються. Складність майнінгу визначає, наскільки важко знайти новий блок та отримати винагороду. Вона залежить від алгоритму майнінгу та кількості майнерів у мережі.

5. Регулювання: Криптовалюти підлягають різному правовому регулюванню в різних країнах. Деякі країни приймають сприятливі регуляторні політики щодо криптовалют, інші обмежують або забороняють їх використання. Регулювання може стосуватися оподаткування, визнання криптовалюти як законних платіжних засобів, боротьби зі злочинністю тощо.

6. Стабільність: Криптовалюти, особливо більш відомі, такі як Bitcoin, Ethereum і Tether, можуть мати варіації в ціні, що викликає нестабільність. Проекти стабільних монет, таких як USD Coin і Dai, пропонують стабільні криптовалюти, які пов'язані з фіатними валютами, такими як долар США.

Важливо зазначити, що технічні та правові характеристики криптовалют можуть змінюватися з часом, оскільки це ще нова та розвиваюча галузь. Різноманіття і властивості криптовалют визначаються як їх технологічними особливостями, так і правовим середовищем, в якому вони функціонують.

Криптовалюти базуються на криптографічних принципах, таких як притаманні блокчейну, та існує розподілена система реєстрації (DLT). Технічна відповідність означає, наскільки ефективно та безпечно використовується технологія криптовалюти. Основні характеристики, які можуть впливати на технічну відповідність, включають швидкість транзакцій, масштабованість мережі, рівень безпеки, приватність та інші технічні параметри. Правова відповідність означає, наскільки криптовалюта відповідає законодавству тієї країни, де вона використовується. Правовий статус криптовалюти різний у різних країнах. Деякі країни визнають криптовалюти як законний засіб платежу, інші мають обмеження або повну заборону щодо використання криптовалют. Для правової відповідності важливі аспекти включають регулювання ICO (ініціалізація монет), біржових операцій, оподаткування криптовалюти та захист прав споживачів. Фінансова відповідність відноситься до економічної стабільності та прийняття криптовалюти на фінансових ринках. Це включає ліквідність криптовалюти, її вартість, стійкість до волатильності та можливості використання як засіб платежу та зберігання вартості. Соціальна відповідність означає, наскільки криптовалюта відповідає соціальним потребам та цінностям користувачів. Це може включати доступність та простоту використання, переваги в порівнянні з традиційними фіатними валютами, вплив на фінансову інклюзію та можливості розширення фінансових послуг.

Слід зауважити, що другою популярною криптовалютою після Bitcoin є Ethereum, де теж використовуються ДД.

Ethereum представляє собою децентралізовану платформу, поверх якої можна розгорнути децентралізовані програми [7, с. 109]. Смарт-контракт (smart contract, розумний контракт) – це програма, яка виконується виключно так, як запрограмовано, без будь-якої можливості простою, цензури, шахрайства та втручання третьої сторони [8, с. 150]. Смарт-контракти для платформи Ethereum можуть бути написані на різних мовах програмування, включаючи Solidity, LLL та Serpent. Зазначимо, що найбільш популярною стала мова Solidity. Ethereum має внутрішню валюту, яка називається ефір (ether). Для того, щоб розгорнути на платформі смарт-контракт або викликати його методи, нам потрібний ефір. Може існувати кілька екземплярів смарт-контракту або додатка, і кожен екземпляр ідентифікується за його унікальною адресою. Як рахунки користувачів, так і смарт-контракти можуть зберігати

ефір. Фактично Ethereum заснований на структурі даних блокчейну та протоколі консенсусу з доказом виконання роботи. Метод смарт-контракту може бути викликаний через транзакцію або через інший метод. У мережі є два типи вузлів: майнери та звичайні вузли. Звичайні вузли просто зберігають копію блокчейна, а майнер будують блокчейн, виробляючи блоки. Для створення облікового запису Ethereum нам потрібна пара асиметричних ключів.

Ключі шифрування можуть генеруватися з урахуванням різних алгоритмів. Ethereum використовує криптографію на еліптичних кривих (Elliptic Curve Cryptography, ECC) [9, с. 177]. Алгоритм ECC має різні параметри, від яких залежить швидкість та безпека. В Ethereum використана еліптична крива *secp256k1*. Занурення в ECC і його параметри потребують серйозних математичних знань, але в цьому немає необхідності, якщо будують децентралізовані додатки на основі Ethereum, оскільки Ethereum використовує 256-бітове шифрування, а відкритим та закритим ключами Ethereum є 256-бітові числа. Фахівці добре знають, що процесор не може обробити настільки великі числа цілком, їх представляють у вигляді шістнадцяткового рядка з 64 символів.

Кожен обліковий запис представлений адресою. Коли є ключі, то потрібно генерувати адресу. Процедура генерації адреси відбувається так:

1. Генеруємо хеш відкритого ключа алгоритмом *keccak-256*. Це дає вам 256-бітне число.
2. Відкидаємо перші 96 бітів (12 байтів) – тепер у вас має залишитися 160 бітів (20 байтів).
3. Потім кодуємо адресу в шістнадцятковий рядок. Отже, ви отримали рядок із 40 символів – це і є ваша адреса.

Після цього будь-хто може перевести ефір на цю адресу. Приведений вище опис необхідний для розуміння криптовалют в цілому. Без нього неможливо обговорювати криптовалюту, в тому числі й в юридичній літературі. При цьому велике значення має сама транзакція – підписаний пакет даних, призначений для переміщення ефіру з одного рахунку на інший рахунок або в контракт, виклик методу контракту або розгортання нового договору. Транзакція має бути підписана цифровим підписом ECDSA (Elliptic Curve Digital Signature Algorithm, алгоритм цифрового підпису на еліптичних кривих). Транзакція містить покажчик на одержувача повідомлення, підпис відправника, що підтверджує його особу та наміри, кількість ефіру для передачі, максимальна кількість обчислювальних кроків, дозволених для виконання транзакції (так званий ліміт газу), та вартість, яку відправник транзакції готовий заплатити за кожен обчислювальний крок (так звана ціна газу). Якщо призначення транзакції полягає у виклику методу контракту, вона також містить вхідні дані, і якщо вона призначена для розгортання контракту, може містити код ініціалізації. Кількість газу та його вартість називаються збором за транзакцію. Щоб надіслати ефір або виконати метод контракту, вам необхідно транслювати транзакцію до мережі. Відправник повинен підписати транзакцію за допомогою закритого ключа. Транзакція вважається підтвердженою, якщо ми впевнені, що вона назавжди залишилася у блокчейні. Рекомендується зачекати 15 підтверджених блоків, перш ніж вважати транзакцію підтвердженою. Це пов'язано з тим, що існує ймовірність, що транзакція стане недійсною, якщо мережа дістане угоди. А це може статися, коли недійсним є блок транзакцій, що вже поміщений

у блокчейн. Скасування більше 15 блоків поспіль технічно неможливе через величезний обсяг обчислень.

Кожен вузол у мережі Ethereum зберігає копію реєстру транзакцій. Ми маємо бути впевнені, що вузол не втрутився у блокчейн, і нам потрібний механізм перевірки достовірності блоків. А також, якщо ми зіткнемося з двома різними дійсними блокчейнами, у нас має бути спосіб дізнатися, який із них вибрати.

Ethereum використовує протокол із доказом виконання роботи, щоб захистити блокчейн від фальсифікації. Принцип доказу роботи передбачає створення нового блоку рішення складної обчислювальної задачі. Рішення завдання має вимагати витрачання значних обчислювальних ресурсів, що робить створення нового блоку складною роботою. Процес створення нового блоку називається майнінгом. Майнерами тут виступають вузли мережі, які виробляють нові блоки. Усі децентралізовані додатки, які використовують доказ виконання роботи не використовують абсолютно однаковий набір алгоритмів. Вони можуть відрізнитися в деталях щодо того, яке завдання має вирішити майнер, наскільки складним має бути завдання, скільки часу займає рішення і т. п. Ми розглядатимемо алгоритм доказу роботи стосовно до Ethereum. Будь-який учасник мережі може стати майнером. Кожен майнер вирішує завдання індивідуально. Перший майнер, який вирішив завдання, стає переможцем і отримує п'ять ефірів та збори від усіх транзакцій, що увійшли до блоку. Якщо ваш процесор потужніший, ніж у решти вузлів мережі, це не означає, що ви завжди будете переможцем, тому що параметри завдання не однакові для всіх майнерів. Однак, якщо ваш процесор потужніший, у вас більше шансів на успіх. Алгоритм доказу роботи схожий на лотерею, а обчислювальна потужність процесора відповідає кількості куплених лотерейних білетів. Безпека мережі залежить немає кількості майнерів, як від сукупної обчислювальної потужності мережі.

Не існує обмеження щодо кількості блоків у блокчейні та за кількістю ефіру, що можна виробити. Як тільки майнер створив блок, він транслює його всім іншим вузлам мережі. Блок містить заголовок та набір транзакцій. Кожен блок містить хеш попереднього блоку, утворюючи нерозривний ланцюг.

Висновки. Юридичні питання щодо дослідження криптовалют, включаючи питання їх подальшого розвитку, без достатнього розуміння того, про що йдеться у цій статті, в прийнятному обсязі вирішити майже неможливо. Важко аналізувати та виявляти механізми взаємодії (управління процесами) в таких складних системах як криптовалюта, а також їх юридично осмислювати. Такий стан предмету, що обговорюється, потребує застосування міжгалузевих знань. Отже, дослідження криптовалюти, як важливого інструменту світового господарства в епоху цифрових технологій (з урахуванням задач господарського та цивільного права), потребують розуміння предмета та основ, на яких він базується. А це неможливо без обговорення реального функціонування блокчейн-технології, оскільки не можна обговорювати те, чого недостатньо розумієш. З цієї причини серед опублікованих юридичних статей з тематики криптовалют є лише незначна кількість наукових праць, в яких є розуміння поняття «блокчейн», що тягне за собою недостатнє розуміння проблем крипто валюти в цілому, як з наукової, так і з практичної точки зору. В цій площині стає очевидною необхідність подальших дослідницьких розробок у цій галузі.

ЛІТЕРАТУРА

1. Cryptocurrency. URL: <https://en.wikipedia.org/wiki/Cryptocurrency>.
2. Бойко В. Д., Василенко М. Д., Новіков В. П., Рачук В. О. «Розумне місто» в контексті розвитку технологій блокчейн. *Комунальне господарство міст. Серія: технічні науки та архітектура*. Харків, 2021. Вип. 3 (163). С. 152–158.
3. Бойченко Е. Г., Могил Л. С. Щодо функцій криптовалют та їх вплив на розвиток господарських правовідносин. *Юридичний науковий електронний журнал*. 2023. № 4. С. 247–250.
4. Закон України № 2074-IX «Про віртуальні активи» від 17.02.2022. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>

5. Milashovska, O., Liba, N., Korolovych, O., Smyrnova, N., & Slatvinska, V. (2022). The potential of applying blockchain technologies in various sectors of the digital economy. *Journal of the University of Zulia*, 13(36), 288–304. DOI: <https://doi.org/10.46925//rdluz.36.19>. URL: <https://produccioncientificaluz.org/index.php/rluz/article/view/37558>
6. Slatvinska Valeria, Demchenko Vitaliia, Tretyak Kateryna, Hnatyuk Rostyslav, Yarema Oleg (2022). The Impact of Blockchain Technology on International Trade and Financial Business. *Universal Journal of Accounting and Finance*, 10(1), 102–112. DOI: 10.13189/ujaf.2022.100111. Scopus. Q4 URL: <https://www.hrpub.org/download/20211230/UJAF11-12225490.pdf>
7. Золотарьова І. О. Інформаційні технології оптимізації роботи приватного блокчейн за допомогою вибору алгоритму консенсусу. Системи обробки інформації : зб. наук. праць. Х. : ХУПС ім. І. Кожедуба, 2020. Вип. 1. С. 107–114.
8. Іванов А.М., Шмига В.О. Смарт-контракти у договірних відносинах: реалії та перспективи використання. *Юридичний науковий електронний журнал*. 2023. № 4. С. 150–152. DOI: <https://doi.org/10.32782/2524-0374/2022-4/32>
9. Гнатюк С.О., Кінзерявий В.М., Поліщук Ю.Я., Нечипорук О.П., Горбаха Б.М. (2022). Аналіз методів забезпечення конфіденційності даних, які передаються з БПЛА. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 1(17), 167–186. <https://doi.org/10.28925/2663-4023.2022.17.167186>