

УДК 347.2

DOI [https://doi.org/10.36919/3041-1149\(Print\)14.2026.186-193](https://doi.org/10.36919/3041-1149(Print)14.2026.186-193)

Ю. О. Подолян,

кандидат юридичних наук, доцент,

доцент кафедри транспортного права

факультету соціально-економічних та правових наук,

Національний транспортний університет

email: yulia29p@gmail.com

ORCID 0000-0001-5063-4018

ВІРТУАЛЬНИЙ АКТИВ У ЦИВІЛЬНОМУ СПОРІ: ВСТАНОВЛЕННЯ НАЛЕЖНОСТІ ТА ОЦІНЮВАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ

VIRTUAL ASSET IN A CIVIL DISPUTE: ESTABLISHING ENTITLEMENT AND ASSESSING ELECTRONIC EVIDENCE

Статтю присвячено особливостям доказування в цивільних і господарських спорах, предметом яких є віртуальні активи. Встановлено, що запис у розподіленому реєстрі достовірно відображає технічні параметри операції, проте сам собою не ідентифікує учасника правовідносин і не розкриває правову підставу набуття активу. Проаналізовано вимоги процесуального законодавства України до форми, належності, допустимості та достовірності електронних доказів, а також практику Верховного Суду, Принципи УНІДРУА щодо цифрових активів і рішення в справі *ByBit FinTech Ltd v Ho Kai Xin*. Запропоновано послідовність встановлення юридично значущих обставин: індивідуалізація активу й операції; встановлення зв'язку особи з адресою або обліковим записом; перевірка правової підстави належності; підтвердження цілісності та походження цифрових даних; оцінювання узгодженості технічних і позацифрових доказів у сукупності. Обґрунтовано, що демонстрація доступу до гаманця, скріншот блокчейн-оглядача або паперова копія електронного повідомлення не повинні мати наперед визначеної доказової сили. Наукова новизна полягає в розробленні фактологічно-доказової моделі, яка поєднує технічну верифікацію операції з процесуальним встановленням особи та матеріально-правовою підставою вимоги. Запропоновано використовувати паспорт електронного доказу, що містить мінімальний набір даних про джерело, спосіб одержання, часову прив'язку, контрольну суму, збереження оригіналу й можливість незалежного відтворення результату.

Ключові слова: віртуальний актив, електронні докази, цифровий слід, розподілений реєстр, блокчейн-транзакція, ідентифікація, належність активу, достовірність доказів, оцінювання доказів, цивільний спір.

The article examines proof in civil and commercial disputes involving virtual assets. It establishes that a distributed-ledger record reliably reflects the technical parameters of a transaction but does not, by itself, identify a party to the legal relationship or disclose the legal basis for acquiring the asset. The study analyses Ukrainian procedural requirements governing the form, relevance, admissibility and reliability of electronic evidence, as well as the case law of the Supreme Court of Ukraine, the UNIDROIT Principles on Digital Assets and Private Law, and *ByBit FinTech Ltd v Ho Kai Xin*. It proposes a sequence for establishing legally relevant facts: individualising the asset and the transaction; linking a person to an address or account; verifying the legal basis of entitlement; confirming the integrity and provenance of digital data; and assessing technical and off-chain evidence as a coherent



whole. Demonstrating access to a wallet, presenting a blockchain-explorer screenshot, or submitting a paper copy of an electronic message should not have predetermined evidentiary weight. The scientific novelty lies in a fact-and-evidence model that combines technical verification of the transaction with procedural identification of the person and the substantive legal basis of the claim. The article proposes an electronic-evidence passport recording the source, method of acquisition, timestamp, hash value, preservation of the original, and the possibility of independently reproducing the result.

Keywords: *virtual asset, electronic evidence, digital trace, distributed ledger, blockchain transaction, identification, asset entitlement, reliability of evidence, assessment of evidence, civil dispute.*

Постановка проблеми. Віртуальний актив існує та обертається в цифровому середовищі, тому спір щодо його належності майже завжди переносить суд у площину електронних доказів. У розподіленому реєстрі можна встановити адресу відправника й одержувача, час, обсяг і послідовність операцій, однак ці відомості не дають безпосередньої відповіді на питання, яка фізична чи юридична особа діяла за відповідною адресою, на якій правовій підставі вона одержала актив і чи зберігся первинний цифровий матеріал без змін. Процесуальні кодекси відносять до електронних доказів не лише електронні документи, а й вебсторінки, повідомлення, метадані, бази даних та іншу інформацію в цифровій формі [1, ст. 100; 2, ст. 96]. Отже, складність полягає не у відсутності можливих джерел інформації, а в правильному визначенні того, яку саме обставину підтверджує кожне з них і в якому взаємозв'язку ці джерела мають оцінюватися.

На практиці сторони нерідко подають до суду скріншот блокчейн-оглядача, роздруківку кабінету біржі або демонструють можливість підписати повідомлення певним ключем і вважають це достатнім для підтвердження належності активу. Такий підхід поєднує різні предмети доказування: існування запису, технічну можливість розпорядитися активом, ідентифікацію конкретної особи та правову підставу для її вимоги. Наслідком може бути як необґрунтоване визнання вимоги, так і відмова в захисті лише через те, що цифрові дані подано у формі, яка не дає змоги перевірити їх автентичність. З огляду на це актуальним є вироблення практичної послідовності збирання та оцінювання доказів, придатної для вирішення спорів про повернення активу, виконання договору, спадкування, відшкодування шкоди, корпоративне використання гаманця або зобов'язання постачальника кастодіальних послуг.

Аналіз останніх досліджень і публікацій. Загальні критерії оцінювання електронних доказів у цивільному процесі досліджено В. П. Фенничем, який звертає увагу на труднощі встановлення їхньої належності, допустимості та достовірності, зокрема в справах, пов'язаних із криптовалютою [7, с. 370–375]. М. Жушман обґрунтовує значення первинних метаданих, хеш-значень, часових міток і документування ланцюга збереження цифрового матеріалу [8, с. 172–178]. Правову природу цифрової речі висвітлено Т. І. Бровченко та Д. Є. Білоусом [9, с. 25–30], а договірну модель зберігання віртуальних активів – А. Г. Донець [10, с. 40–63]. Питання моменту набуття права власності за цивільно-правовим договором і правового режиму власності аналізують В. В. Посполітак, Є. Ю. Савченко [11; 12].

Наявні праці сформували відповідну матеріально-правову та процесуальну основу, проте для судового спору залишається недостатньо розробленим порядок переходу від технічного запису до висновку про юридично значущу обставину. Практика Верховного Суду наголошує на можливості оцінювати електронне листування, коли можна встановити його учасників і зміст, обов'язково в сукупності з іншими матеріалами [13]. У міжнародному вимірі Принципи УНІДРУА допускають ідентифікацію особи, яка здійснює контроль за номером, криптографічним ключем, офісом або обліковим записом, навіть якщо такий ідентифікатор не розкриває її імені [16, Principle 7]. Це положення є корисним для технічної верифікації, але потребує процесуального доповнення доказами, що пов'язують цифровий ідентифікатор із конкретним учасником спору.

Метою статті є формування послідовної моделі встановлення належності віртуального активу в цивільному спорі та оцінювання пов'язаних із ним електронних доказів, для чого визначено обставини, які входять до предмета доказування, розмежовано первинні цифрові дані та їхні похідні візуальні відображення, окреслено способи встановлення зв'язку між особою, адресою та обліковим записом, узагальнено вимоги до збереження та перевірки цілісності матеріалу й

запропоновано матрицю доказування як практичний інструмент, за допомогою якого суд і сторони можуть оцінити взаємну узгодженість технічних та позацифрових доказів.

Виклад основного матеріалу дослідження. Відповідно до статей 177 та 179-1 ЦК України цифрові речі належать до об'єктів цивільних прав, а їхній правовий режим визначається законом з урахуванням сутності відповідного блага [5]. Закон України «Про віртуальні активи», який станом на 2026 рік не набрав чинності, пов'язує віртуальний актив із нематеріальним благом, що є об'єктом цивільних прав, має вартість і виражене сукупністю даних в електронній формі [6]. Для доказування це означає, що відомості про актив розосереджені між кількома інформаційними середовищами: розподіленим реєстром, програмним гаманцем, обліковою системою постачальника послуг, електронним листуванням, банківськими документами та договорами. Жодне із цих середовищ не повинно автоматично вважатися основним: їхнє доказове значення залежить від обставини, для встановлення якої відповідні дані подаються.

Першим кроком має бути точна індивідуалізація активу та спірної операції. Для нативної криптовалюти варто зазначити мережу, адресу або набір адрес, ідентифікатор транзакції (TxID), висоту блоку, час внесення до блоку, вид і кількість одиниць. Для токена додатково фіксуються адреса смартконтракту, стандарт токена та, якщо йдеться про невзаємозамінний актив, його token ID. У разі обміну, мосту або обгортання активу потрібно показати пов'язані операції в кожній мережі. Саме така деталізація дає іншій стороні й суду змогу повторити пошук у незалежному оглядачі та перевірити, чи стосується поданий матеріал того самого цифрового об'єкта. Посилання лише на назву монети, баланс гаманця або зображення екрана не забезпечує належної індивідуалізації.

Запис у публічному реєстрі підтверджує, що протокол прийняв операцію як належно авторизовану відповідно до його технічних правил. Водночас адреса є протокольним ідентифікатором, а не іменем учасника цивільних відносин. Принцип 7 УНІДРУА слушно визнає криптографічний ключ або номер облікового запису допустимим засобом ідентифікації в межах системи, не вимагаючи, щоб він розкривав ім'я особи [16, Principle 7]. На нашу думку, у судовому доказуванні потрібні дві послідовні операції: спочатку встановити, яка адреса або обліковий запис пов'язаний з операцією, а потім – якими зовнішніми даними цей цифровий ідентифікатор пов'язується з конкретною фізичною чи юридичною особою. Пропуск другого етапу перетворює технічно правильний висновок на юридично неповний.

До початку збирання матеріалів доцільно скласти карту «обставина, доказ, спосіб перевірки». У типовому спорі вона охоплює: існування та індивідуальні ознаки активу; факт, час і маршрут операції; зв'язок кожної релевантної адреси з учасником; правову підставу виникнення вимоги; збереження первинних даних; обставини, якими опонент пояснює іншу належність або інший зміст операції. Для кожної позиції потрібно зазначити не лише джерело, а й спосіб незалежної перевірки. Наприклад, TxID перевіряється за даними кількох вузлів або оглядачів, належність біржового облікового запису – за реєстраційними даними та журналами входу, а договірна підстава – за договором, платежем, листуванням і поведінкою сторін після виконання. Така карта запобігає накопиченню значної кількості однотипних скріншотів, які не закривають ключової прогалини в предметі доказування.

За способом утворення матеріали в справі доцільно поділяти на первинні цифрові дані, їхні технічні вибірки та візуальні відображення. До першої групи належать дані вузла мережі, журнали подій платформи, файл електронного повідомлення з повними заголовками, підписаний файл або експорт історії операцій. Друга група охоплює звіт аналітичного програмного забезпечення, таблицю вибраних транзакцій або експертний висновок. Третя – скріншот, роздруківку або відеозапис перегляду. Похідний матеріал може бути зрозумілішим для суду, але не замінює джерела, з якого його отримано. Тому до кожного звіту чи зображення потрібно додавати відомості про використаний сервіс, версію або дату доступу, пошукові параметри й місце збереження первинного масиву.

Процесуальна форма подання електронного доказу має самостійне значення. ЦПК України та ГПК України передбачають подання оригіналу або електронної копії, засвідченої електронним підписом; допускається й паперова копія, яка, однак, не перетворюється на письмовий доказ

[1, ст. 100; 2, ст. 96]. Якщо оригінал не подано, а відповідність копії оригіналу обґрунтовано поставлено під сумнів, суд може не брати її до уваги. Закон України «Про електронні документи та електронний документообіг» водночас забороняє заперечувати юридичну силу чи допустимість документа виключно через його електронну форму [3, ст. 8]. Отже, проблема полягає не в самій роздруківці або скріншоті, а в тому, чи можна зіставити їх з доступним оригіналом і перевірити спосіб одержання. Такий підхід узагальнено і в огляді практики Верховного Суду [15, слайди 1–3].

Дані блокчейн-оглядача можуть розглядатися як відображення відомостей із вебсторінки або бази даних, але інтерфейс оглядача не є самим розподіленим реєстром. Його зміст може змінюватися через оновлення сервісу, вибір часової зони, позначення токенів, фільтрацію внутрішніх операцій або помилкове визначення мережі. Тому під час фіксації потрібно зберегти повну URL-адресу, дату й точний час доступу, назву мережі, TxID, номер блока, використані фільтри, експорт доступних даних і повносторінкове відображення. Якщо спір має значну вартість, доцільно одержати ті самі відомості з іншого незалежного джерела або безпосередньо з вузла. Збіг результатів не створює наперед визначеної сили доказу, проте істотно підвищує його перевірюваність.

Актуальний доступ до некастодіальної адреси можна встановити через підписання нейтрального повідомлення або виконання погодженої мікротрансакції. Така дія має містити індивідуальний текст, номер справи та часову позначку, щоб унеможливити повторне використання старого підпису. Водночас суд не повинен вимагати розкриття приватного ключа або seed phrase, оскільки це створює ризик втрати активів. Варто також урахувати межі висновку: коректний підпис підтверджує здатність скористатися відповідним засобом авторизації у визначений момент, але не доводить, хто створив попередню трансакцію, як особа отримала доступ і на якій правовій підставі заявляє вимогу. За схемами мультипідпису або розподіленого обчислення потрібно окремо описати кількість відповідних підтверджень і роль кожного учасника.

Для кастодіального гаманця основне доказове значення часто мають не ключі, а дані постачальника послуг: реєстраційні та KYC-відомості, історія зміни контактів, журнали входу, ідентифікатори пристроїв та IP-адрес, налаштування багатофакторної автентифікації, адреси виведення, заявки на переказ і службове листування. Оскільки строки зберігання таких даних можуть бути обмеженими, сторона має невідкладно звернутися із запитом про їхнє збереження, а за потреби – клопотати до суду про їхнє витребування. Показовою є справа *ByBit FinTech Ltd v Но Kai Xin*, у якій зв'язок відповідачки з гаманцем підтверджувався реєстраційними даними, документом, що посвідчує особу, фотографією та записами операцій постачальника послуг [17, paras. 25, 41]. Саме поєднання незалежних категорій даних зробило висновок переконливим.

Наступним кроком є перевірка матеріально-правової підстави вимоги. Вона може впливати з договору купівлі, міни, дарування чи зберігання, спадкування, внесення активу до майна юридичної особи, виплати винагороди, повернення безпідставно набутого або відшкодування шкоди. Технічний переказ повинен відповідати договору, рахунку, банківському платежу, умовам платформи, корпоративним рішенням, спадковим документам і листуванню сторін. Дослідження договору зберігання віртуальних активів показує залежність обсягу обов'язків постачальника від обраної моделі послуги [10, с. 40–63], а момент набуття права за договором потребує зіставлення волі сторін із фактичним виконанням [11]. Тому наявність активу за адресою є лише одним елементом, а не заміною правової підстави.

Достовірність цифрового матеріалу значною мірою залежить від способу його збереження. Доцільно зберігати первинний файл або експорт у форматі, в якому він був одержаний, окремо фіксувати метадані, обчислювати хеш-значення й вести журнал кожного копіювання чи передання. Для електронного документа важливо зберегти обов'язкові реквізити, а для повідомлення – повні технічні заголовки та вкладення [3, ст. 5–7]. Кваліфікована електронна позначка часу або інша довірча послуга може підтвердити існування даних у певний момент, якщо її застосовано відповідно до законодавства [4]. М. Жушман слушно відносить метадані, хеші, часові мітки та документований ланцюг збереження до мінімальних елементів перевірюваності цифрового сліду [8, с. 172–178]. Ці дії не гарантують правдивості змісту, але дають змогу виявити подальші зміни.

Залучення експерта є доцільним, коли без спеціальних знань неможливо відтворити маршрут активу, перевірити підпис, дослідити файл гаманця, журнали пристрою або ознаки втручання. Питання мають бути технічними: чи відповідає TxID певній операції; чи пов'язані вказані адреси послідовністю переказів; чи змінювався файл після визначеної дати; чи створено підпис ключем, відповідним зазначеній адресі; які дані зберігаються на пристрої. Не потрібно доручати експерту визначати власника активу, правомірність набуття або достовірність пояснень сторони – це правове оцінювання суду. Висновок має містити джерела даних, застосовані інструменти, їхні версії, параметри пошуку та проміжні результати, щоб інший фахівець міг відтворити дослідження.

Відповідно до статті 89 ЦПК України та статті 86 ГПК України жоден доказ не має наперед встановленої сили; суд оцінює належність, допустимість і достовірність кожного доказу окремо, а достатність і взаємний зв'язок – у сукупності [1; 2]. Для спору щодо віртуального активу це правило має особливе значення. Переконливий висновок виникає тоді, коли дані реєстру, ідентифікаційні відомості платформи, документи про правову підставу, фінансовий слід і поведінка сторін підтверджують одну версію подій, а виявлені розбіжності мають розумне пояснення. Суду доцільно окремо зазначати в рішенні, яку обставину доводить кожне джерело, які заперечення щодо нього перевірено та чому сукупність матеріалів переважає альтернативну версію.

Практика Верховного Суду підтверджує потребу саме в такому підході. Велика Палата в справі № 916/3027/21 зазначила, що електронне листування може бути прийняте як доказ, якщо з огляду на конкретні обставини воно дає змогу встановити учасників і підтвердити відповідні доводи; оцінювати його потрібно разом з іншими доказами [13]. Об'єднана палата Касаційного господарського суду в справі № 914/1003/21 розмежувала електронний документ та електронний доказ і вказала, що подання паперової копії саме собою не робить електронний доказ недопустимим [14, пп. 67–71]. Наведені висновки можуть бути застосовані й до блокчейн-даних: форма їхньої візуалізації не вирішує наперед питання допустимості, якщо походження, зміст і відповідність оригіналу можуть бути перевірені.

Ілюстративною для запропонованої моделі є справа *ByBit FinTech Ltd v Ho Kai Xin*. Суд не обмежився фактом переказу USDT на чотири адреси. Було досліджено службові таблиці із заміненіми адресами одержувачів, видалені електронні листи, реєстраційні дані гаманця, записи подальших транзакцій, пояснення відповідачки та її витрати, які не узгоджувалися із заявленою версією [17, paras. 8–17, 25]. На підставі сукупності прямої та непрямої інформації суд за стандартом балансу ймовірностей визнав доведеною причетність відповідачки [17, para. 41]. Цей приклад показує, що блокчейн-аналітика стає юридично переконливою не через складність технології, а через узгодження з даними про особу, службовими повноваженнями, фінансовою поведінкою та спростуванням альтернативних пояснень.

У спорі про виконання прямого переказу позивачеві недостатньо показати вихід активу зі своєї адреси. Потрібно індивідуалізувати операцію, довести погодження адреси одержувача, правову мету платежу та зв'язок відповідача з цією адресою. Такий зв'язок може підтверджуватися повідомленням, у якому було надано адресу, попередніми операціями між тими самими сторонами, підписаним повідомленням, даними біржі або подальшим розпорядженням активом. Відповідач, заперечуючи належність адреси, має пояснити походження переписки, збіг реквізитів та інші об'єктивні обставини. Якщо адреса була помилково замінена шкідливим програмним забезпеченням, предмет доказування доповнюється даними пристрою, часом підміни й повідомленнями сторін одразу після операції.

У справах про викрадення або несанкціонований переказ особливого значення набуває хронологія цифрових подій. Потрібно зіставити час входу до гаманця чи біржового кабінету, зміну паролів і засобів автентифікації, IP-адреси та пристрої, повідомлення про операцію, звернення до постачальника послуг, подальший маршрут активу й момент подання заяви компетентним органам. Демонстрація доступу після події не доводить, що та сама особа створила спірну транзакцію раніше; так само відсутність доступу після переказу не підтверджує автоматично факт викрадення. На нашу думку, суд повинен оцінювати швидкість і послідовність реакції сторони разом із технічними даними, не перетворюючи поведінку після події на самостійний вирішальний доказ.

Спiр iз бiржею або iншим кастодiальним постачальником потребує врахування того, що баланс у кабiнетi клiєнта може вестися у внутрiшнiй базi даних i не вiдповiдати окремiй адресi в публiчному реєстрi. У такому разi недостатньо аналізувати лише агрегованi гаманцi постачальника. Дослiдженню пiдлягають умови послуги, внутрiшня iсторiя зарахувань i списань, заявки на виведення, журнали пiдтверджень, полiтика розподiлу адрес, звітнiсть про резерви та листування служби пiдтримки. Зiставлення внутрiшнього запису з конкретною on-chain операцiєю має здiйснюватися за сумою, часом, мережею, адресою депозиту або iдентифiкатором, який постачальник присвоїв цiй операцiї. Договiрна природа вiдносин i технiчна архiтектура сервісу визначають, якi саме данi вiн має зберiгати та надавати [10].

Для корпоративного або службового гаманця особа, яка технiчно пiдтвердила операцiю, не обов'язково є самостiйною стороною матерiального правовiдношення. Потрiбно дослiдити статутнi та внутрiшнi документи, розподiл повноважень, накази, полiтику зберiгання ключiв, порядок погодження платежiв, журнали системи мультипiдпису та посадовi обов'язки працівника. Якщо пiдпис формують кiлька осiб, доказове значення має не лише кiнцевий запис у реєстрi, а й послiдовнiсть внутрiшнiх погоджень. Такий пiдхiд дає змогу вiдрiзнити технiчне виконання доручення вiд самовiльної операцiї та встановити, чи дiяла особа в межах наданих їй повноважень. Аналогiчно в спадковому спорi технiчний доступ спадкоємця пiсля смертi власника не замiнює доказiв складу спадщини та прийняття спадщини.

Збереження доказiв має передувати їхньому докладному аналізу, оскiльки частина даних є мiнливою або зберiгається лише на обмежений час. У заявi про забезпечення доказiв чи клопотаннi про витребування доцiльно точно називати мережу, адреси, TxID, облiковий запис, часовий промiжок i категорiї журналiв, а не просити надати «всю iнформацiю про криптовалюту». Для постачальника послуг окремо зазначаються KYC-данi, iсторiя входiв, змiни реквiзитiв, заявки на виведення, адреси призначення та листування з пiдтримкою. Водночас обсяг запиту має бути пропорцiйним предмету спору й не передбачати розкриття приватних ключiв. Чiткiсть предмета витребування пiдвищує ймовiрнiсть фактичного виконання ухвали та зменшує ризик отримання масиву, який неможливо спiввiднести з обставинами справи.

Для унiфiкацiї фiксацiї пропонується додавати до кожного ключового цифрового матерiалу паспорт електронного доказу. Вiн має мiстити: найменування джерела й власника iнформацiйної системи; опис способу та дати одержання; iдентифiкатори активу, операцiї або облiкового запису; назву й версiю використаного програмного засобу; формат i мiсце збереження оригiналу; хеш-значення файлу або набору даних; вiдомостi про кожне копiювання; спiсiб незалежного вiдтворення; обмеження, що впливають на iнтерпретацiю результату. Паспорт не є новим видом доказу й не пiдмiняє засвiдчення копiєю. Його призначення – зробити зрозумiлим походження матерiалу та шлях вiд первинних даних до висновку, на який посилається сторона. Схожий технiчний мiнiмум узгоджується з пропозицiями щодо метаданих, хешiв i ланцюга збереження [8, с. 172–178].

Наукова новизна запропонованого пiдходу полягає у фактологiчно-доказовiй моделi вирiшення спору щодо вiртуального активу. Її основою є не надання переваги одному технiчному iндикатору, а послiдовний перехiд вiд iндивiдуалiзацiї операцiї до встановлення особи, вiд встановлення особи до перевiрки правової пiдстави, а вiд окремих джерел – до оцiнювання їхньої цiлiсностi та взаємної узгодженостi. Модель дає змогу локалізувати доказову прогалину: наприклад, запис пiдтверджує маршрут активу, але немає даних про особу; KYC iдентифiкує власника кабiнету, але не пояснює конкретну операцiю; договiр фiксує обов'язок, але його виконання не збiгається з даними реєстру. Саме виявлення такої прогалини визначає, який додатковий доказ потрiбно витребувати або дослiдити.

Висновки. Спiр щодо вiртуального активу не може бути вирiшений лише через перенесення даних розподiленого реєстру до тексту судового рiшення. Реєстр надiйно фiксує технiчну операцiю в межах вiдповiдного протоколу, але не розкриває повнiстю особу учасника та правову пiдставу його вимоги. Тому запис, скрiншот, пiдписане повiдомлення, KYC-вiдомостi, договiр i платiжний документ повиннi оцiнюватися вiдповiдно до обставин, якi кожен iз них може пiдтвердити.

За результатами проведеного дослідження запропоновано п'ять послідовних етапів доказування: індивідуалізація активу й операції; встановлення зв'язку особи з адресою або обліковим записом; перевірка матеріально-правової підстави належності; підтвердження походження, цілісності та збереження цифрових даних; оцінювання узгодженості технічних і позацифрових доказів у сукупності. Пропуск будь-якого етапу не завжди робить вимогу недоведеною, але має бути прямо врахований судом під час зіставлення конкурентних версій подій.

Сторонам доцільно зберігати первинні електронні дані, повні метадані та технічні заголовки, фіксувати хеш-значення й часові позначки, а похідні звіти супроводжувати описом способу їхнього отримання. Суду потрібно уникати вимоги про розкриття приватного ключа, формулювати технічні питання експерту та окремо мотивувати, яку обставину доводить кожне джерело. Запропонований паспорт електронного доказу може слугувати практичним чек-листом без запровадження нового процесуального засобу доказування.

Перспективним є розроблення Верховним Судом або органами суддівського врядування методичних рекомендацій щодо мінімального складу фіксації блокчейн-даних, витребування відомостей у постачальників послуг і меж експертного дослідження. Такі рекомендації мають залишатися технологічно нейтральними та спиратися на чинні правила належності, допустимості, достовірності й сукупного оцінювання доказів. Це сприятиме однаковому підходу до цифрових матеріалів без надання їм наперед встановленої сили.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цивільний процесуальний кодекс України : Закон України від 18 березня 2004 р. № 1618-IV. URL : <https://zakon.rada.gov.ua/laws/show/1618-15#Text>
2. Господарський процесуальний кодекс України : Закон України від 6 листопада 1991 р. № 1798-XII. URL : <https://zakon.rada.gov.ua/laws/show/1798-12#Text>
3. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 р. № 851-IV. URL : <https://zakon.rada.gov.ua/laws/show/851-15#Text>
4. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII. URL : <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
5. Цивільний кодекс України : Закон України від 16 січня 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40–44. Ст. 356. URL : <https://zakon.rada.gov.ua/laws/show/435-15#Text>
6. Про віртуальні активи : Закон України від 17 лютого 2022 р. № 2074-IX (не набрав чинності станом на 18.08.2026). URL : <https://zakon.rada.gov.ua/laws/show/2074-20#Text>
7. Феннич В. П. Оцінка електронних доказів у цивільному процесі (на прикладах окремих категорій судових справ). *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. Вип. 71. С. 370–375. DOI : <https://doi.org/10.24144/2307-3322.2022.71.63>
8. Жушман М. Цифровий слід як джерело доказів у цивільному судочинстві України: національний та міжнародний виміри. *Інформація і право*. 2025. № 4 (55). С. 172–178. DOI : [https://doi.org/10.37750/2616-6798.2025.4\(55\).346388](https://doi.org/10.37750/2616-6798.2025.4(55).346388)
9. Бровченко Т. І., Білоус Д. Є. Цифрова річ як новий об'єкт цивільних прав. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки*. 2024. Т. 35 (74), № 1. С. 25–30. DOI : <https://doi.org/10.32782/TNU-2707-0581/2024.1/05>
10. Донець А. Г. Договір зберігання віртуальних активів (Crypto Custody) за законодавством України. *Теорія і практика правознавства*. 2022. Вип. 2 (22). С. 40–63. DOI : <https://doi.org/10.21564/2225-6555.2022.2.267943>
11. Посполітак В. В., Савченко Є. Ю. Момент набуття права власності на віртуальні активи за цивільно-правовим договором. *Київський часопис права*. 2025. № 4. С. 57–63. DOI : <https://doi.org/10.32782/kjp/2025.4.8>
12. Савченко Є. Ю. Правовий режим власності на віртуальні активи. *Нове українське право*. 2024. № 6. С. 165–181. DOI : <https://doi.org/10.51989/NUL.2024.6.24>
13. Постанова Великої Палати Верховного Суду від 21 червня 2023 р. у справі № 916/3027/21, провадження № 12-8гс23. URL : <https://reyestr.court.gov.ua/Review/112088045>

14. Постанова Об'єднаної палати Касаційного господарського суду у складі Верховного Суду від 15 липня 2022 р. у справі № 914/1003/21. URL : https://supreme.court.gov.ua/supreme/pro_sud/rishennya_obedn_palati_kgs_vs/2022_07_15_914_1003_21
15. Уркевич В. Використання електронних доказів у господарському процесі: практика Верховного Суду. *Треті наукові читання пам'яті професора Пронської Грацієлли Василівни* : Міжнародна науково-практична конференція, 12 квітня 2024 року / Київський національний університет імені Тараса Шевченка. URL : https://www.supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2024_prezent/Prezent_Vukor_eletr_dokaziv_gosp_proc_2024.pdf
16. Principles on Digital Assets and Private Law / UNIDROIT. Rome, 2023. URL : <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf>
17. ByBit FinTech Ltd v Ho Kai Xin and others [2023] SGHC 199. Judgment of 25 July 2023. URL : https://www.elitigation.sg/gd/s/2023_SGHC_199

Дата надходження статті: 03.07.2026

Дата прийняття статті: 26.08.2026

Дата публікації статті: 14.09.2026