УДК 347.2; 346.3;347.1
DOI https://doi.org/10.32782/2524-0374/2025-9/36

ПРАВОВІ АСПЕКТИ ПОСВІДЧЕННЯ ПРАВОЧИНІВ, ВЧИНЕНИХ ЗА ДОПОМОГОЮ СМАРТ-КОНТРАКТІВ

LEGAL ASPECTS OF THE TRANSACTION'S AUTHENTICATION EXECUTED VIA SMART CONTRACTS

Тищенко А.В., аспірант кафедри економічного права та економічного судочинства
Навчально-науковий інститут права Київського національного університету імені Тараса Шевченка
радник,
Адвокатське об'єднання «Арцінгер»

У статті досліджуються правові аспекти посвідчення правочинів, вчинених за допомогою смарт-контрактів, у контексті сучасного розвитку цифрових технологій та цифровізації господарського обороту. Актуальність теми зумовлена потребою визначення меж легітимності цифрового підпису в блокчейн-середовищі та його співвідношення з традиційними засобами електронної ідентифікації та автентифікації.

Автор акцентує увагу на співвідношенні між традиційними формами електронного підпису, зокрема кваліфікованим електронним підписом (КЕП), та криптографічним підписом, який використовується для підтвердження транзакцій у блокчейн-середовищі. Здійснено комплексний аналіз нормативно-правових підходів України, ЄС, США та міжнародних актів (зокрема Регламенту eIDAS та Типового закону UNCITRAL про електронні підписи), що дозволяє зіставити юридичні гарантії автентичності, цілісності та незаперечності підпису у різних правових системах.

Окрема увага приділяється технічним особливостям застосування функціонування системи відкритих і приватних ключів, процедурі формування цифрового підпису, а також відмінностям між централізованими системами сертифікації та децентралізованими механізмами блокчейну. Підкреслюється, що криптографічний підпис у блокчейні фактично виконує ті самі базові функції, що і КЕП, проте відсутність централізованої сертифікації та формальної процедури ідентифікації унеможливлює його офіційне прирівнювання до КЕП без відповідних законодавчих змін.

Автор доходить висновку, що криптографічний підпис у блокчейні наразі може кваліфікуватися щонайменше як простий електронний підпис, тоді як його легалізація в українському законодавстві можлива шляхом унормування моделі взаємного визнання та інтеграції процедур KYC/AML у правове регулювання Web3.

Практичне значення дослідження полягає у виробленні рекомендацій для адаптації українського законодавства до нових викликів децентралізованої економіки та формуванні правових засад для майбутньої інтеграції блокчейн-технологій у систему електронного документообігу.

Ключові слова: смарт-контракт, електронний підпис, блокчейн, криптографічний підпис, КЕП, Web3, правочин.

The article examines the legal aspects of certifying transactions concluded through smart contracts in the context of the digitalization of commercial relations and the rapid development of blockchain technology. The relevance of the topic is determined by the need to delineate the boundaries of digital signatures legitimacy within the blockchain environment and to assess their correlation with traditional instruments of electronic identification and authentication.

The author focuses on the correlation between traditional forms of electronic signatures, in particular the qualified electronic signature (QES), and the cryptographic signature, used to authenticate transactions in blockchain systems. A comparative analysis of the regulatory approaches of Ukraine, the European Union, the United States, and international instruments (including the EU eIDAS Regulation and the UNCITRAL Model Law on Electronic Signatures) is conducted to assess the legal guarantees of authenticity, integrity, and non-repudiation of signatures across different jurisdictions.

Special attention is given to the technical features of the functioning of public and private key systems, the procedure of digital signature generation, as well as the differences between centralized certification infrastructures and decentralized blockchain mechanisms. It is emphasized that the cryptographic signature in blockchain in fact performs the same fundamental functions as the Qualified Electronic Signature (QES), however, the absence of centralized certification and a formal identification procedure precludes its official recognition as equivalent to the QES without the adoption of corresponding legislative amendments.

The study highlights that while blockchain-based signatures perform the same core functions as QES, the absence of centralized certification prevents their recognition as fully equivalent to QES under current Ukrainian law. The paper argues that blockchain signatures can already be qualified at least as simple electronic signatures (SES), and their legalization within Ukrainian law is possible through the introduction of mutual recognition models and the integration of KYC/AML procedures into the regulation of Web3 interactions.

The practical significance of the research lies in developing recommendations for adapting Ukrainian legislation to the challenges of decentralized economy and creating a legal foundation for integrating blockchain technologies into the system of electronic document circulation.

Key words: smart contract, electronic signature, blockchain, cryptographic signature, QES, Web3, transaction.

Вступ. Стрімка цифровізація господарських правовідносин зумовлює необхідність переосмислення традиційних підходів до оформлення правочинів, підписання договорів і забезпечення їх юридичної чинності. Електронний підпис давно перетворився на невід'ємний атрибут електронного документообігу та електронних послуг у всьому світі. Зокрема, кваліфікований електронний підпис (КЕП) в Україні та ЄС за правовим статусом прирівнюється до власноручного підпису.

Водночас новітні технології, такі як блокчейн, породили такі феномени як смарт-контракти, віртуальні та токенізовані активи. У смарт-контрактах юридично значущі дії (наприклад, передання активів, емісія токенів, тощо) відбуваються після застосування «цифрового підпису» для посвідчення транзакції учасником операції. Проте правова природа та легітимність такого підпису в смарт-контрактах залишається невизначеною через відсутність прямого нормативного регулювання і усталеної правозастосовної практики.

У даній статті пропонується комплексний порівняльний аналіз електронного цифрового підпису та підпису, що використовується у смарт-контрактах, з акцентом на їх криптографічну природу, юридичний статус, практичне застосування виклики та перспективи правового регулювання.

Результати дослідження.

1. Нормативно-правове регулювання використання ЕЦП.

Проблематика волі і волевиявлення давно перебуває в центрі уваги правової доктрини. Такі українські правники, як О. В. Дзера, О. А. Беляневич, В .В. Резнікова, Н. С. Кузнєцова, В. С. Мілаш, І. В. Спасибо-Фатєєва, В. М. Коссак, О .Г. Харитонова, С. В. Бичкова та інші, у своїх працях так чи інакше підкреслювали необхідність єдності внутрішньої волі особи і її зовнішнього волевиявлення для чинності правочину.

Водночас, питання складу, термінології, правового статусу ЕЦП, порядок його застосування досліджували І. Я. Верес, О. В. Костенко, О. А. Дрогозюк, О. А. Присяжнюк, С. В. Губарєв, О. О. Лов'як, Р. В. Новосад та інші.

Актуальність дослідження полягає у відсутності належного правового врегулювання порядку посвідчення правочинів у блокчейн-середовищі, адже смарт-контракти дедалі ширше застосовуються у господарському обороті, але статус їх підписання не має чіткого правового визначення в українському законодавстві.

За загальним правилом, волевиявлення є належним, якщо воно одночасно відповідає кільком умовам:

1) наявність у особи внутрішньої волі на вчинення правочину, яка передбачає усвідомлення особою характеру своїх дій та бажання настання їх правових наслідків (особа має розуміти, що вона робить, який саме правочин укладає, з яким контрагентом, на яких умовах і який результат бажає отримати). Відсутність внутрішньої волі означає, що правочин кваліфікується як фіктивний або удаваний;

2) наявність свободи волевиявлення та відсутності дефектів волі (помилки, обману, насильства, зловмисної домовленості, тяжких обставин тощо).

3) зовнішнє вираження волі має бути зрозумілим, чітко зафіксованим і таким, що не викликає сумніву щодо змісту волі. В письмовій формі таке волевиявлення виражається у проставленні власноручного підпису, який виконує функцію відображення наміру особи на досягнення результату та є частиною ідентифікуючих ознак особи, яка його підписала. Водночас, коли мова йде про електронний договір, то загальноприйнятим посвідченням волі особи є використання електронного цифрового підпису («ЕЦП»).

В українському законодавстві поняття ЕЦП було вперше визначено Законом України «Про електронний цифровий підпис», за яким ЕЦП визнається аналогом власноручного підпису за умови дотримання встановлених вимог, крім того документ із накладеним ЕЦП не може бути визнаний недійсним лише через те, що він має електронну форму.

З розвитком права Європейського Союзу (ЄС) відбулася гармонізація підходів до електронного підпису. Регламент ЄС № 910/2014 (eIDAS) запровадив поняття «кваліфікованого електронного підпису» (КЕП), який відповідає підвищеним вимогам безпеки. Згідно з eIDAS, лише КЕП має таку саму юридичну силу, як і власноручний підпис. Втім, на рівні з ним, Регламент eIDAS також виділяє простий та удосконалений електронні підписи [1].

Верховна Рада України поступово імплементувала європейські стандарти, прийнявши Закони України «Про електронні документи та електронний документообіг» [2], «Про електронні довірчі послуги» [3] (згодом Закон України «Про електронну ідентифікацію та електронні довірчі послуги» («Закон про ЕЦП»)) та «Про електронну комерцію» [4].

Закон про ЕЦП визначив аналогічний до eIDAS термін КЕП замість ЕЦП (який визначався ще першим Законом України «Про електронний цифровий підпис», прийнятий у 2003 році), привівши таким чином українське законодавство у відповідність до європейського.

Законодавством України визначено 3 категорії електронного цифрового підпису, які можуть посвідчувати той чи інший правочин, вчинений у електронній формі, однак, які різняться між собою у рівні надійності та доказовості зв'язку між підписантом та документом, на який «накладається» підпис, а також достовірністю змісту самого документа. Так:

1) *електронний підпис (простий або спрощений електронний підпис «ПЕП»)* – електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис (п. 15 ч. 1 ст. 1 Закону про ЕЦП);

2) *удосконалений електронний підпис (УЕП)* (згідно ст. 17-1 Закону про ЕЦП), повинен відповідати наступним ознакам: (1) однозначно пов'язаний з підписувачем; (2) дозволяє ідентифікувати підписувача; (3) створюється за допомогою особистого ключа, який знаходиться під повним контролем підписувача; (4) пов'язаний з підписаними даними так, що будь-яку їх зміну можна виявити;

3) *КЕП* – є удосконаленим електронним підписом, що створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті електронного підпису (п. 27 ч. 1 ст. 1 Закону про ЕЦП). КЕП це найвищий рівень електронного підпису, який, окрім вимог, що визначені для УЕП також має 2 додаткові вимоги: (1) має базуватись виключно на кваліфікованому сертифікаті, виданому довіреним надавачем; (2) його особистий ключ має зберігатись у спеціальному захищеному засобі КЕП (наприклад, захищений токен чи апаратний пристрій).

Після того, як eIDAS зобов'язав всі держави-члени ЄС визнавати КЕП, створені в інших країнах-членах, і не вимагати в публічному секторі підписів вищого рівня, ніж КЕП, в Європі було сформовано єдиний правовий режим, за яким КЕП визнається єдиним презюмовано достовірним і рівноцінним власноручному підпису. Це значно спростило транскордонний електронний документообіг та сприяло розвитку електронних послуг. З 2023 року Україна фактично приєдналась до такої системи, згідно якої КЕП, видані в ЄС, є еквівалентними українським КЕП (аналогічно тому, як країни ЄС визнають українські КЕП на території ЄС). Згодом, постановою Кабінету Міністрів України «Про внесення змін до постанов Кабінету Міністрів України від 11 серпня 2023 р. № 844 і від 14 листопада 2023 р. № 1198 та визнання такими, що втратили чинність, деяких постанов Кабінету Міністрів України» від 01.10.2024 р. № 1131, також було погоджено взаємне визнання довірчих списків кваліфікованих надавачів довірчих послуг.

При цьому, варто відрізняти електронний підпис від ЕЦП. Зокрема, як відзначають С. В. Губарєв та О. О. Лов'як, ЕЦП є видом електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність і ідентифікувати підписувача. Електронний цифровий підпис накладається та перевіряється за допомогою відкритого ключа [5, с. 22].

Натомість, до ПЕП відносяться не тільки ЕЦП, але і:

– *одноразовий ідентифікатор* – дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору (ст. 12 Закону України «Про електронну комерцію»). По суті, таким підписом є введення одноразового коду (ОТР), що підтверджує намір особи укласти електронний договір;

– *заповнення формуляра заяви (форми)*. Як відзначає В. С. Мілаш, акцепт електронної оферти може здійснюватися також шляхом заповнення формуляра заяви (форми) про прийняття пропозиції в електронній формі

або вчиненням дій, що вважаються прийняттям пропозиції укласти електронний договір, якщо зміст таких дій чітко роз'яснено в інформаційній системі, в якій розміщено таку пропозицію, і ці роз'яснення логічно пов'язані з нею. При цьому, крім істотних умов для відповідного виду договору, згідно до ст. 11 Закону України «Про електронну комерцію», сам електронний договір може містити інформацію про порядок його укладення. Це означає, що якщо на рівні законодавчого регулювання не висунуто спеціальної вимоги щодо порядку укладення конкретного виду господарського договору, такий порядок може визначатися на рівні договірного регулювання [6, с. 35];

– *натискання позначки «погоджуюсь»* (договори «*click-wrap*» – договори, при укладанні яких акцепт здійснюється кліком [7, с. 88]) також може фіксувати акцепт як простий електронний підпис за умови належної ідентифікації та фіксування дій користувача;

– *використання скановаого зображення підпису*, як аналога власноручного підпису, можливе лише у випадках, передбачених законом або за письмовою угодою сторін із визначенням зразків.

Для порівняння, нормативно-правове врегулювання цього питання в США засноване на дещо іншій концепції. Основними актами є федеральний закон «Electronic Signatures in Global and National Commerce Act» (E-SIGN Act) [8] та прийнятий у більшості штатів Єдиний закон про електронні транзакції (UETA) [9], які не поділяють електронні підписи на прості на «кваліфіковані» чи «удосконалені». Натомість діє технологічно нейтральний підхід, згідно якого, електронний підпис визначається дуже широко – як «електронний звук, символ або процес, прикріплений чи логічно поєднаний з контрактом або іншим записом і виконаний або прийнятий особою з наміром підписати цей запис» (що наближено за змістом до ПЕП в Україні, зокрема, у формі одноразового ідентифікатора чи інший узгоджений спосіб). Втім, на відміну від підходу eIDAS, в США закон фактично надає електронному підпису та електронному документу ту саму юридичну силу, що й паперовим, і встановлює, що жодному підпису чи контракту не може бути відмовлено в юридичній силі, чинності або виконуваності лише тому, що він виконаний в електронній формі.

Тобто, у США електронний підпис визнається повноцінним способом вираження волі, якщо сторони надали відповідну згоду на електронну взаємодію (для цього, E-SIGN містить вимоги щодо отримання згоди споживачів на електронний формат, можливості збереження копій тощо). Втім, такий підхід не визначає конкретні технічні засоби підпису: це може бути і цифровий підпис (на основі криптографії), і просте натискання кнопки «*Я згоден*», і введення імені тощо. Ключовими є лише вимоги щодо наявності: (1) наміру особи надати згоду на здійснення правочину (укладення договору) та (2) зв'язку такої згоди (підпису) із конкретним документом.

Як відзначає О. В. Костенко, фактично держава відходить від регулювання процедури визнання електронних послуг, електронних підписів та сертифікатів і покладає це на суб'єктів-учасників правовідносин, адже одним із принципових положень UETA є норма, згідно якої визнання дійсності електронних угод, електронних документів, електронних підписів та їх сертифікатів можливі за згодою сторін, що беруть участь у обміні електронними документами [10, с. 81]. Така гнучкість сприяла масовому впровадженню електронних підписів у господарських правовідносинах, хоча викликає питання надійність і доказовість такого способу електронного підписання документів.

Свій підхід визначила також Комісія ООН з міжнародного торгового права UNCITRAL, розробивши спеціальний Типовий закон UNCITRAL про електронні підписи («Типовий закон»). Стаття 2 Типового закону визначає понятійно-термінологічний апарат, в якості основних, що стосуються проблематики дослідження, можна виокремити наступні:

1) *електронний підпис* – дані в електронній формі, що містяться у повідомленні даних, прикріплені до нього або логічно з ним пов'язані, які можуть бути використані для ідентифікації підписувача у зв'язку з повідомленням даних та для засвідчення згоди підписувача з інформацією, що міститься у повідомленні даних;

2) *сертифікат* – повідомлення даних або інший запис, що підтверджує наявність зв'язку між підписантом і даними для створення підпису;

3) *повідомлення даних* – інформація, створена, надіслана, отримана або збережена електронними, оптичними чи подібними засобами, включаючи, але не обмежуючись, електронним обміном даними (EDI), електронною поштою, телеграмою, телексом або телекопією.

В п. 29 Посібника по прийняттю типового закону UNCITRAL про електронні підписи («Посібник UNCITRAL»), визначено ключові функції, які традиційно покладаються на власноручний підпис, а саме: (1) ідентифікація особи, (2) забезпечення визначеності у відношенні до особистої участі особи у процесі підписання і (3) підтвердження цією особою змісту документа. Крім того, також відмічаються такі побіжні / допоміжні функції, як: підтвердження наміру сторони бути пов'язаною із змістом підписаного контракту; намір особи погодити авторство будь-якого тексту (проявляючи тим самим розуміння того, які правові наслідки акт підписання може нести); намір особи погодитись із змістом документу, написаного іншою особою; факт, що будь-яка особа під час підписання знаходилась у місці та часі підписання. Ці ж ознаки фактично мають переноситись на ЕЦП [11].

Незважаючи на те, що вищезгадані нормативно-правові акти по-різному визначають вимоги для прирівнювання ЕЦП до власноручного підпису, на нашу думку спостерігається певний консенсус в частині ключових функцій та ознак які доказують факт посвідчення особою тих чи інших документів, умов договору чи даних в електронному вигляді. Так, незмінними є вимоги до того, що ЕЦП має забезпечувати:

1) належну автентифікацію підписанта за допомогою засобів електронної ідентифікації (матеріальних та/або нематеріальних об'єктів, які містять ідентифікаційні дані особи і використовується для автентифікації особи в інформаційно-комунікаційних системах);

2) цілісність документа або електронних даних (будь-якої інформації у електронній формі);

3) невідмовність підписанта від факту підписання документа саме з тим змістом, який було посвідчено підписом (зв'язок між документом і засобами електронної ідентифікації, який посвідчує волевиявлення особи).

Звідси виникає питання щодо того чи відповідає спосіб посвідчення операцій в мережі блокчейн вищезазначеним законним вимогам до ЕЦП та способам підписання електронних договорів в Україні?

Для цього, варто проаналізувати технічні особливості та відмінності накладення визнаних в Україні способів підписання договорів в електронній комерції від підпису, прийнятного для смарт-контрактів.

2. **Особливості накладення ЕЦП на документ.**

Згідно положень Закону про ЕЦП, створення та використання ЕЦП базується на методах криптографічного захисту, адже саме вони здатні відповідати ключовим вимогам до належного посвідчення правочинів: (1) здійснення перевірки справжності (ідентифікація) відправника (одержувач зашифрованого файлу може переконатись, що особа, яка його відправила – є саме тим відправником, яким має бути. Водночас, зловмисник не дає можливості маскуватися під справжнього відправника); (2) здійснення перевірки цілісності документа (отримувач документа, може перевірити факти відсутності несанкціонованої

модифікації інформації / тексту, а зловмисник не може видати підроблений текст за справжній); (3) доказовість та незаперечіність авторства підпису та контроль підписанта на особистим ключем (відправник не може заперечувати підписання документа) [12, с. 163].

Виходячи із системного аналізу положень Закону про ЕЦП та п. 36 Посібника UNCITRAL, ЕЦП вибудовується на принципах асиметричних систем криптографічного захисту (систем з відкритим ключем або двоключових систем).

Інфраструктура відкритих ключів (англ. *Public key infrastructure, «PKI»*) – це інтегрований комплекс методів та засобів (наборі служб), призначених забезпечити впровадження та експлуатацію криптографічних систем із відкритими ключами [12, с. 197]. Технологія PKI відзначається як на рівні UNCITRAL, eIDAS та Закону про ЕЦП, та полягає у використанні пари ключів: відкритого та особистого (див. п. 41 ч. 1 ст. 1 Закону про ЕЦП)). Саме їх визначення наводяться у пунктах 5 ч. 1 ст. 1 Закону про ЕПЦ: (1) *особистий ключ* (дані для створення електронного підпису чи печатки) – унікальні дані, що використовуються підписувачем чи створювачем електронної печатки для створення електронного підпису чи печатки; (2) *відкритий ключ* (дані для підтвердження електронного підпису чи електронної печатки) – дані, що використовуються для підтвердження електронного підпису чи електронної печатки.

За своєю сутністю, відкритий та особистий (приватний) ключі – є унікальними наборами символів (чисел і літер), сформованих у результаті роботи криптографічних алгоритмів. Важливо те, що з особистого ключа обчислити публічний легко, в той час як з публічного обчислити приватний практично неможливо (це забезпечує безпеку доступу до нього) (див. п. 36-39 Посібника UNCITRAL).

Для того, щоб посвідчити чинність публічного ключа, необхідно щоб центр сертифікації сформував сертифікат відкритого ключа – прив'язав до публічного ключа основні атрибути підписувача, а саме: ім'я та ідентифікатор суб'єкта, інформація про відкритий ключ суб'єкта, ім'я, ідентифікатор і цифровий підпис уповноваженого з видачі сертифікатів, серійний номер, версія і термін дії сертифіката, інформація про алгоритм підпису тощо. Важливо, що цифровий сертифікат містить цифровий підпис на основі секретного ключа довірчого центру [12, с. 198].

Відповідно до положень ст. ст. 13 та 20 Закону про ЕЦП, виключно кваліфікований надавач електронних довірчих послуг, засвідчувальний центр чи центральний засвідчувальний орган може надавати послуги, що належать до переліку кваліфікованих електронних довірчих послуг. Кваліфікована електронна довірча послуга з формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає: (1) створення умов для генерації пари ключів особисто підписувачем чи створювачем (уповноваженим представником створювача) електронної печатки за допомогою засобу кваліфікованого електронного підпису чи печатки; (2) формування кваліфікованих сертифікатів електронного підпису чи печатки, що відповідають вимогам цього Закону, та видачу їх користувачу електронної довірчої послуги; (3) скасування, блокування та поновлення кваліфікованих сертифікатів електронного підпису чи печатки у випадках, передбачених цим Законом; (4) перевірку та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки шляхом надання третім особам інформації про їхній статус та відповідність вимогам цього Закону; (5) надання доступу до сформованих кваліфікованих сертифікатів електронних підписів та печаток шляхом їх розміщення на офіційному веб-сайті кваліфікованого надавача електронних довірчих послуг, за умови згоди підписувача чи створювача електронної печатки на публікацію кваліфікованого сертифіката електронного підпису чи печатки.

Маючи таку інфраструктуру відкритих ключів, процес підписання будь-якого електронного документа (накладення приватного ключа) проходить декілька етапів:

1) *хешування документа.* Спеціальне програмне забезпечення сканує зміст документа (порядок розміщення букв, цифр і символів, що містяться в документі), та перетворює цей зміст у певний унікальний «відбиток» – «хеш» (короткий рядок символів фіксованої довжини). Якщо зловмисник захоче підробити зміст документа, навіть зміна хоча б одного символа – зумовить повну трансформацію хешу (короткий рядок символів повністю зміниться на інший). Саме зміна хеша свідчить про підробку змісту документа;

2) *підписання хеша особистим ключем*. Особистий ключ використовується, щоб «зашифрувати» хеш документа за певним криптографічним алгоритмом (RSA, ECDSA тощо). В результаті, зашифрований хеш документа видається у вигляді математичного блоку даних, що являє собою електронний цифровий підпис;

3) *формування «контейнера» з інформацією у спеціальному форматі для зчитування*. Отримані результати поміщаються у файл, який містить в собі: (1) оригінал підписаного документа, (2) електронний підпис – зашифрований хеш, (3) сертифікат підписувача (відкритий ключ з даними підписувача) та (4) технічну службову інформацію (часові мітки застосування підпису (timestamp), алгоритми шифрування, політика підпису, ідентифікатори, тощо).

Отримувач файла може за допомогою спеціального програмного забезпечення (ПЗ) здійснити перевірку цілісності документа за наступним алгоритмом: ПЗ знову формує «відбиток» змісту оригінального документа (вираховує хеш за тим же алгоритмом, за яким він формувався при підписанні) та порівнює результат із хешем, який міститься в контейнері. У разі їх відповідності ПЗ підтверджує незмінність оригінального змісту документа.

Таким чином, особистий ключ використовується для шифрування документів, які можуть бути розшифровані тільки за допомогою другого (публічного) ключа. При цьому, відкритий ключ – відкритий для всіх (за його допомогою інші особи можуть звірити особу підписанта посвідченого документа особистим ключем), а особистий ключ має приватний характер і повинен зберігатись в захищеному місці (тобто має бути доступний безпосередньо та виключно підписанту).

Вказана система, забезпечує значно вищу технічну гарантію того, що підпис неможливо буде підробити (на відміну від власноручного), однак його недолік полягає в тому, що у разі отримання доступу сторонньої особи до особистого ключа – встановити дефект волевиявлення з технічної точки зору буде неможливо. Тому, діюче законодавство ЄС та України фактично презюмує той факт, що доступ до особистого ключа наявний виключно у належної особи (хоч така презумпція є умовною).

3. Особливості виклику (запуску) функцій смарт-контрактів у блокчейн-середовищі.

Згідно із вже класичним визначенням, запропонованим Ніком Сабо, смарт-контракт розглядається як комп'ютерний протокол, що самостійно забезпечує виконання умов договору при настанні визначених у середовищі блокчейну обставин. Фактично, смарт-контракти та блокчейн середовище загалом побудовані на тих ще принципах та методах криптографічного захисту, що і ЕЦП.

Водночас, як відзначають О. Клепікова, О. Гарагонич та І. Антошина, для того щоб смарт-контракт був юридично еквівалентним звичайному договору, який має обов'язкову силу, він повинен відповідати критеріям, встановленим цивільним законодавством, зокрема правилам укладення угод (дійсність правочинів). Аналіз практики вітчизняного та зарубіжного законодавства у цьому

аспекті показує, що смарт-контракти мають перспективу застосування у різних сферах життя, однак для цього вони повинні відповідати вимогам закону, що не завжди є оптимальним для смарт-контрактів [13, с. 856]. Це стоється і питання коректного їх підписання.

Враховуючи те, що на відміну від традиційного договору, смарт-контракт укладається і виконується не у вигляді текстового документа, а як алгоритм, розміщений у розподіленому реєстрі (блокчейні), з технічної точки зору, звичні способи його використання поки що не передбачають можливості його запуску (підписання) безпосереднім накладенням власноручного підпису або ЕЦП. А відтак, питання його запуску (підписання) особливо гостро постає з точки зору права.

Для встановлення відповідності та легальності його укладення з позицій українського та європейського законодавства, необхідно проаналізувати технічну сторону підписання смарт-контракту через призму вищенаведених правил та принципів посвідчення електронних договорів.

Процес взаємодії сторін через смарт-контракт, детально досліджувався у роботі таких дослідників як Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, Muhammad Imran у своїй статті ґрунтовно описують механізм технічної взаємодії сторін через смарт-контракт без участі третіх осіб. Приділено увагу автоматизації виконання угод і механізму виклику функцій та виконання алгоритмів контракту [14, с. 3–4].

Так, зокрема, зазначається про те, що у механізм та логіка роботи смарт-контракту відображає наступні технічні моменти, які за своєю суттю мають багато подібного до вищеописаного механізму створення та використання ЕЦП:

1) *генерація пари ключів:* будь-які операції у Web3[1] потребують криптографічної пари ключів (аналогічно ЕЦП). Приватний ключ створюється як випадкове число, з нього математично виводиться публічний ключ, а шляхом хешування виводиться – адреса крипто-гаманця. Адреса крипто-гаманця виконує функцію унікального ідентифікатора користувача в мережі блокчейн (аналог номеру банківського рахунку), тоді як публічний ключ застосовується для перевірки автентичності цифрових підписів. Приватний ключ може зберігатися: (1) у зашифрованому вигляді у пам'яті застосунку (наприклад, MetaMask, TrustWallet), (2) на апаратному носії (Ledger, Trezor), (3) у вигляді мнемонічної seed-фрази (12–24 слова), що дає можливість відновити доступ до гаманця;

2) *ініціювання транзакції*: для приєднання до умов смарт-контракту (акцепту оферти), користувач викликає функцію контракту (наприклад, «buyTokens(amount)» чи «stake(deposit)») через інтерфейс веб-сайту, застосунку або іншого ПЗ. Для цього у гаманці формується запит із зазначенням відправника (адреси користувача), одержувача (адреси іншої сторони або контракту), суми чи інструкції (аналогічно тому, як відповідні платежі проводяться у банківській системі);

3) *підпис особистим ключем*: для підтвердження транзакції користувач застосовує свій особистий (приватний) ключ, який створює унікальний цифровий підпис (хеш транзакції). Це підтверджує його авторство та цілісність даних, що є аналогом електронного підпису в правовому обігу;

4) *виконання алгоритму*: підписана транзакція надсилається до блокчейн-мережі, де після верифікації вона виконує закладений у смарт-контракт алгоритм (наприклад, перерахунок токенів від підписанта до іншої сторони чи блокування депозиту на адресі смарт-контракту). Результат операції фіксується у розподіленому реєстрі шляхом включення інформації про транзакцію до блоку блокчейну. Цей запис є незмінним завдяки механізму консенсусу та криптографічному зв'язуванню блоків. Умовно це можна порівняти з тим, як у системах електронного документообігу інформація про ЕЦП зберігається у спеціальному файлі-контейнері, що забезпечує перевірку автентичності та цілісності даних.

Як видно із етапів застосування підпису у блокчейн-середовищі, його функціонал є близьким до порядку підписання документів за допомогою ЕЦП. Однак, чи відповідає такий підпис визначеним вище вимогам законодавства відносно порядку посвідчення правочинів, вчинених в електронному вигляді. Для цього, необхідно проаналізувати його відповідність ознакам та властивостям КЕП.

4. Відповідність підпису у Web3 вимогам законодавства України.

Аналізуючи процес посвідчення правочинів, вчинених у Web3 за допомогою смарт-контрактів, варто зосередити увагу на наступних правових аспектах підпису:

1) *ідентифікація відправника*: цифровий підпис транзакцій в смарт-контракті, аналогічно до КЕП, створюється приватним ключем, завдяки чому мережа має змогу перевірити його коректність через відповідний публічний ключ/адресу. Це гарантує, що транзакція дійсно походить від власника ключа та контролера адреси крипто-гаманця;

Водночас, на відміну від КЕП, у Web3 відсутній сертифікаційний центр, який офіційно засвідчив би особу власника ключа. Тобто система може підтвердити справжність ключа, але не ідентифікує особу, що ним користується, адже у Web3 основним ідентифікатором підписанта виступає «деперсоніфікована адреса крипто-гаманця».

Цю проблему можна частково вирішити шляхом закріплення конкретних адрес за фізичними чи юридичними особами – учасниками правочину. Це можливо, зокрема, через біржі та постачальників віртуальних активів, які здійснюють процедури KYC[2] при реєстрації акаунту (персонального кабінету), коли користувач має надати необхідні ідентифікуючі документи (паспорт, водійські права тощо). В інших випадках (у разі невикористання адрес крипто-гаманців на вищезазначених біржах у двосторонніх господарських правовідносинах) це можливо лише через укладення додаткової угоди, у якій сторони прямо вказують адреси своїх гаманців, подібно до погодження використання факсиміле чи сканкопії підпису у класичних договорах.

Водночас, навіть за умови встановлення такого зв'язку підпис у блокчейні не буде повноцінним аналогом КЕП, оскільки для цього потрібно, щоб пара ключів була згенерована та сертифікована уповноваженим кваліфікованим надавачем електронних довірчих послуг. В іншому випадку така пара ключів не визнається офіційно авторизованою, що ставить під сумнів довіру держави до застосованих криптографічних методів, навіть якщо вони фактично забезпечують ті самі функції.

Крім того, сам процес ідентифікації відправника у блокчейні не опосередковується діяльністю будь-якого офіційного органу чи установи, а отже, не має зовнішнього гаранта автентичності.

Втім, слід підкреслити, що результат (наприклад, переказ токенів іншій стороні) у блокчейні досягається не завдяки довірі до конкретного оператора (посередника), а через те, що алгоритм зафіксований у коді смарт-контракту та сама транзакція проходить верифікацію децентралізованою мережею (майнерами чи валідаторами). Це становить ключову відмінність від інфраструктури КЕП в Україні, де верифікація здійснюється цен-

[1] Web3 – концепція нової ітерації розвитку інтернету, який би був децентралізованим та базувався б на блочейнах. URL: https://uk.wikipedia.org/wiki/Web3

[2] KYC (англ. know your customer – знай свого клієнта) – термін банківського та біржового регулювання для фінансових інститутів і букмекерських контор, а також інших компаній, які працюють з грошима приватних осіб, що означає, що вони повинні ідентифікувати та встановлювати особу контрагента, перш ніж проводити фінансову операцію. https://uk.wikipedia.org/wiki/%D0%97%D0%BD%D0%B0%D0%B9_%D1%81%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BA%D0%BB%D1%96%D1%94%D0%BD%D1%82%D0%B0

тралізованими установами. А отже, потреба у створенні такого органу – відпадає сама по собі, оскільки його функцію виконує сама архітектура мережі блокчейн.

2) *перевірка цілісності документа:* транзакція смарт-контракту хешується, і підпис підтверджує саме цей хеш. Будь-яка зміна даних зробить підпис недійсним, що абсолютно відповідає властивості забезпечення цілісності змісту виконаної операції.

Більше того, навіть сам смарт-контракт (що по суті є цифровим договором, який містить умови домовленостей сторін) є незмінним після його деплойменту («розгортання» – процесу завантаження скомпільованого байт-коду смарт-контракту (його умов) у блокчейн, після чого він стає загальнодоступним та його зміна не допускається). Саме ці властивості фактично знімають необхідність перевірки цілісності самого смарт-контракту.

3) *унеможливлення заперечення авторства (незаперечність):* Якщо транзакцію підписано приватним ключем і її включено до ланцюга з належною фінальністю, оспорити авторство (що це підписав не власник ключа) криптографічно неможливо, адже вказана інформація «фіксується» криптографічним ланцюгом хешів, де зміна будь-якого попереднього блоку потребує перерахунку хешів всіх наступних. Більше того, у більшості мереж після певної кількості підтверджень («чекпойнтів») запис вважається остаточним.

Тому, авторство підписанта можливо оспорити лише шляхом доведення того факту, що ключ був скомпрометований або перебував поза контролем підписувача до моменту підписання (наприклад, у разі викрадення seed-фрази, доступу до акаунту на біржі / сервісі або приватного ключа). На відміну від КЕП, у блокчейні немає механізму відкликання підпису заднім числом. Тому, припинити виконання смарт-контракту можна тільки якщо до деплойменту в його код були закладені відповідні запобіжники.

Таким чином, з технічної точки зору підпис у блокчейні відповідає принаймні двом ознакам КЕП із трьох. Натомість, залишаються невирішеними питання ідентифікації особи, яка є фактичним власником крипто-гаманця та сертифікації пари ключів, які генеруються тими чи іншими розробниками Web3 проектів (хоч вони і не є критичними, оскільки за умов надання біржам чи іншим провадерам послуг у сфері Web3 статусу кваліфікованого надавача електронних довірчих послуг, обидві проблеми можуть бути вирішені).

Разом з тим, відповідні умови ставляться виключно в залежність від необхідності кваліфікації підпису в блокченій як КЕП чи власноручного підпису. В той же час, підпис у блокчейні уже цілком підпадає під визначення ПЕП, окресленим вище.

Більше того, у США вже наявні деякі прецеденти кваліфікації такого підпису як електронного. Наприклад, в корпоративному праві штати почали визнавати смарт-контракти як юридично зобов'язуючі. Аризона, Теннессі, Вайомінг – серед лідерів дружнього до блокчейну законодавства, які законодавчо підтвердили, що «смарт-контракт не може бути визнаний недійсним тільки через те, що використовує блокчейн» і що «запис, створений у блокчейні, вважається електронним записом» [15]. Все це створює підґрунтя, на якому використання приватного ключа прирівнюється до електронного підпису у господарських правовідносинах. Однак, у сфері захисту споживачів фінансових послуг в США поки-що немає чітких правил для криптогаманців. Більше того, регулятори як Комісія з цінних паперів і бірж США (SEC) та Комісія з торгівлі товарними ф'ючерсами (CFTC) більше зосереджені на питанні, чи є певні токени цінними паперами, ніж на питанні безпеки гаманців.

Таким чином, важливо враховувати також те, що попри відповідність підпису в блокчен-середовищі формальним ознакам електронного підпису, не варто ігнорувати він не повністю відповідає вимогам законодавства України, які встановлюються для ЕЦП.

Висновки. Проведене дослідження дозволяє зробити наступні теоретико-практичні висновки:

1) будь-який ЕЦП має забезпечувати 3 функції: належну автентифікацію підписанта; цілісність документа; беззаперечність факту підписання документа саме з тим змістом, який було посвідчено ЕЦП конкретного підписанта;

2) криптографічний підпис приватним ключем у блокчейн-середовищі технологічно виконує функції ЕЦП (оскільки забезпечує такі ознаки як автентичність, цілісність, незаперечність), але формально-юридично не може бути аналогом ЕЦП чи власноручного підпису;

3) криптографічний підпис у блокчейн-середовищі може підпадати під ознаки електронного підпису загального типу (ПЕП);

4) для повноцінного юридичного визнання підпису блокчейн-транзакції як волевиявлення особи важливим є встановлення зв'язку між адресою крипто-гаманця та особою, яка здійснює ефективний контроль над гаманцем, а також діями, які відображають намір особи укласти цифровий договір. Зокрема, такий спосіб посвідчення транзакцій, за умови проходження процедури KYC або письмової домовленості сторін. Крім того, система генерації пари ключів (публічного і приватного) має відповідати визначеним державним стандартам;

5) для повноцінної інтеграції крипто-гаманців в правове поле України та легалізації процедури посвідчення за їх допомогою правочинів на рівні власноручного підпису, необхідно реалізувати принаймні наступні зміни:

– ввести в дію Закон України «Про віртуальні активи», адаптований під регламент MiCA – для введення в правове поле систем обміну активами, заснованими на блокчейн механіках та смарт-контрактах.

– доопрацювати законодавство щодо криптогаманців як eID. Зокрема, (1) розширити ст. 15-1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» (eID wallets), щоб включити крипто-гаманці, які зберігають приватні ключі, у перелік засобів електронної ідентифікації з відповідними рівнями довіри; (2) визначити критерії оцінки відповідності таких гаманців з позицій доступу, безпеки, криптографічних стандартів та включити їх до схем eID; (3) надати крипто-біржам та крипто-сервісам можливості ліцензування криптогаманців та їх інтеграції в систему eID.

– нормативно закріпити законність блокчейн-підписів: (1) дати криптографічним підписам у блокчейні (ECDSA від ключів гаманця) статус удосконаленого або кваліфікованого підпису та (2) створити нормативну базу для використання блокчейну як доказу транзакції (з позицій його автентичності, неперервності, та часових міток). Наразі ці аспекти частково можуть бути вирішені на договірній основі між учасниками господарських правовідносин.

– регулювання AML/KYC/ліцензування криптогаманців: введення правил KYC/AML для провайдерів кастодіальних крипто-гаманців, шляхом доповнення положень Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», що може розширити можливості для полегшення ідентифікації власників крипто-гаманців на платформах, які такі політики не вводили.

– передбачити ліцензування або акредитацію провайдерів e-ID крипто-гаманців (подібно до акредитації кваліфікованих надавачів електронних довірчих послуг).

ЛІТЕРАТУРА

1. Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС : Регламент Європейського парламенту і ради (ЄС) від 23 липня 2014 р. № 910/2014. URL: https://zakon.rada.gov.ua/laws/show/984_016-14#Text (дата звернення: 26.08.2025).

2. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 р. № 851-VI (в ред. від 31 грудня 2023 р.). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 26.08.2025).

3. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII (в ред. від 18 грудня 2024 р.). URL: https://zakon.rada.gov.ua/laws/show/2155-19/ed20241218#n7 (дата звернення: 26.08.2025).

4. Про електронну комерцію : Закон України від 3 вересня 2015 р. № 675-VIII (в ред. від 1 січня 2024 р.), URL: https://zakon.rada.gov.ua/laws/show/675-19#n170 (дата звернення: 26.08.2025).

5. Губарєв С.В., Лов'як О.О. Електронний підпис як складова електронних правочинів. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: юридичні науки*. 2022. Т. 33 (72). № 4, С. 18-23, URL: https://www.juris.vernadskyjournals.in.ua/journals/2022/4_2022/3.pdf?utm_source=chatgpt.com (дата звернення: 26.08.2025)

6. Мілаш В.С., Електронні договори як правова основа електронної комерції (торгівлі) в Україні. *Актуальні проблеми права: теорія і практика № 1(43). Вісник Східноукраїнського національного університету імені Володимира Даля*. 2022. С. 33-41, URL: https://journals.snu.edu.ua/index.php/app/article/view/362/343 (дата звернення: 26.08.2025).

7. Філатова Н.Ю. Договори типу Click-Wrap і Browse-Wrap: Особливості і призначення. *Вісник ОНУ імені І.І. Мечникова. Правознавство*. 2018. Т. 23., вип. 1(32), С. 87-97.

8. Electronic Signatures in Global and National Commerce Act : Public Law No. 106-229, June 30, 2000 // Statutes at Large. 114 Stat. 464. URL: https://www.congress.gov/bill/106th-congress/senate-bill/761/text (дата звернення: 26.08.2025).

9. Uniform Electronic Transactions Act. National Conference of Commissioners of Uniform State Laws, July 23-30, 1999.

10. Костенко О.В., Електронний підпис та електронні довірчі послуги в законодавстві Сполучених Штатів Америки // Інформація і право. 2018. № 3(26), С. 76-83. URL: https://ippi.org.ua/sites/default/files/9_9.pdf (дата звернення: 26.08.2025).

11. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. 2001. URL: https://digitallibrary.un.org/record/436958?ln=ru&v=pdf (дата звернення: 26.08.2025).

12. Гончарова Л.Л. та ін. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. Київ. 2013. 435 с. URL: https://web.archive.org/web/20170516180816/http://lib.detut.edu.ua/files/Nauk_trud_vukladahiv/Fakultet%20Infrastruktur_ruxomuy_sklad%20%E2%80%9D/Kafedra_tel_texn_avtomatuka/nauk_trud_voznenko.pdf (дата звернення: 26.08.2025).

13. Klepikova O., Harahonych O., Antoshyna I. Smart contracts in the context of digitalization: the legal realities of world experience. *Cuestiones Politicas*. 2021. Vol. 39, № 70, P. 844-861. URL: https://ippi.org.ua/sites/default/files/9_9.pdf (дата звернення 26.08.2025).

14. Zibin Zheng, Shaoan Xie, and others, An Overview on Smart Contracts: Challenges, Advances and Platforms. URL: https://arxiv.org/pdf/1912.10370 (дата звернення: 26.08.2025).

15. Arizona Revised Statutes. House Bill № 2417, An Act amending section 44-7003, title 44, chapter 26, by adding article 5; relating to electronic transactions. URL: https://legiscan.com/AZ/text/HB2417/id/1497439 (дата звернення: 26.08.2025).

Дата першого надходження рукопису до видання: 29.09.2025
Дата прийнятого до друку рукопису після рецензування: 20.10.2025
Дата публікації: 29.10.2025