УДК 34.01
DOI https://doi.org/10.32849/2663-5313/2020.9.05

Анна Гурова,
канд. юрид. наук, науковий співробітник
Інституту держави і права імені В. М. Корецького
Національної академії наук України

Марія Кірпачова,
керівник юридичного відділу
ТОВ "Space Logistics Ukraine"

ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ БЛОКЧЕЙН У КОСМІЧНІЙ ДІЯЛЬНОСТІ: КЛЮЧОВІ ЕЛЕМЕНТИ ТА МОДЕЛІ ОРГАНІЗАЦІЇ ТЕХНОЛОГІЇ

Стаття є першою із серії публікацій, присвячених дослідженню правової природи технології розподілених реєстрів, зокрема її найпопулярнішого прикладу – технології Блокчейн. Стаття покликана закласти основу для подальшого предметного висвітлення результатів дослідження, пов'язаних із застосуванням технології розподілених реєстрів саме у космічній діяльності та адекватним відображенням вказаних процесів у законодавстві України. У статті подається тлумачення основних елементів технології Блокчейн з юридичної точки зору, аналізуються проблеми, які можуть виникнути у процесі введення цієї технології до правового поля різних галузей господарювання. Таким чином, досліджуються як види самої системи (публічна, приватна, з наявністю чи відсутністю дозволу, методи валідації нових користувачів мережі), так і похідні її інструменти, а саме: смарт-контракти і оракли, а також проблематика їх застосування задля реалізації прав і обов'язків суб'єктів космічної діяльності. Так, зокрема, значна увага приділяється юридичним ознакам смарт-контракту для набуття ним ознак правочину, ідентифікації сторін смарт-контракту для захисту прав категорії менш обізнаних та вразливих користувачів мережі Блокчейн, відповідальності у разі виникнення помилки у програмному коді виконання правочину або навіть у разі втручання в код у результаті кібератак. Водночас детальному вивченню піддається питання криптографічної форми правочину та її визнання на законодавчому рівні. Разом із тим приділяється увага питанню вирішення спорів між сторонами смарт-контрактів, реалістичність уведення до мережі судді або арбітра, а також співвідношення такої ролі з поняттям одноранговості усіх учасників мережі. Крім того, розглядається застосовність інструменту оракл, спрямованого на отримання фіксованих даних із ресурсів за межами мережі, для вирішення проблеми обмеженості мережі при виконанні правочинів. Загалом дослідження демонструє взаємопроникність технічних аспектів функціонування Блокчейн та характер і спектр правовідносин, що нині реалізуються та мають потенціал для реалізації у правовому полі як іноземних держав, так і України.

Ключові слова: Блокчейн, технологія розподілених реєстрів, вузол, однорангові транзакції, токен, хеш-значення, приватний ключ, публічний ключ, валідація, оракл.

Постановка проблеми. Людство пішло шляхом розвитку та інтеграції в космічні та кібернетичні технології. З часу, коли програмне забезпечення почало відігравати ключову роль у наданні космічних послуг, коло суб'єктів космічної діяльності суттєво розширилося, головним чином за рахунок приватних компаній, а самі космічні послуги стали доступними для широкого кола користувачів. Вказане актуалізувало питання щодо пошуку засобів належної організації та захисту інформації. Як відповідь на цей запит нині все частіше пропонується технологія розподілених записів, або її найбільш відомий різновид – Блокчейн. Проте навіть застосування її у валютному секторі, де вона набула найбільшого розвитку, залишається у світі доволі неоднозначним через численні міфи щодо можливостей її застосування, а також дискусійним переважно внаслідок складнощів щодо встановлення загальноприйнятного правового поля для держави, суспільства, бізнесу. Саме ці обставини стали точкою біфуркації, яка спонукала дослідити правові аспекти застосування Блокчейн технології в космічній діяльності крізь призму чотирьох предметних сфер, які стали підґрунтям для 4 самостійних етапів дослідження, присвячених: 1) технології організації Блокчейн та її основним різновидам;

2) космічним послугам, які ця технологія покликана вдосконалити; 3) правовій базі, яка формуватиметься та змінюватиметься для регулювання цієї діяльності; 4) правовим та організаційним засадам державного регулювання космічної діяльності з використанням Блокчейн технологій. Вказана стаття відображатиме результати першого етапу.

Мета статті – дослідити правову природу технології Блокчейн, її основні різновиди.

Аналіз останніх досліджень. Для заглиблення в предмет дослідження авторами було проведено опитування спеціалістів у сфері Блокчейн технології: керуючого партнера Blockchain Lab і викладача курсу Blockchainomics в Києво-Могилянській бізнес-школі Станіслава Подячева, переможниці хакатону BlockchainUA Анастасії Кандаурової. Крім того, досліджено праці О. Дубініної, П. Кравченко, О. Кудь, М. Кучерявенка, Я. Строкової, А. Багмет, М. Рожкової, В. Лебедєва, Б. Скрябіна, Є. Смичка, В. Ляшенко, О. Вишневського, (Distributed Lab), Karen J. Jones, Mohamed Torky, Tarek Gaber, Aboul Ella Hassanien, Rohit Mital, Jack de La Beaujardiere, Rohan Mital, Marge Cole, Charles Norton, Silvia Petruzzino, Manav Gupta, Swapnil Anil Surdi, Jonathan Emmanuel, Nadya Reingand, John Popper, Efraim Turban, Jon Outland, David King, Jae Kyu Lee, Ting-Peng Liang, Deborrah C. Turban тощо. І нарешті, предметом дослідження були акти міжнародного публічного та приватного права, національного законодавства України та зарубіжних держав.

Виклад основного матеріалу. Оскільки навколо Блокчейну є велика кількість міфів, викликаних нечітким розумінням технології, таких як його незламність чи цілковита демократичність, тобто рівність усіх його учасників, спробуємо (без претензії на будь-яку експертність у цій сфері) сформулювати основні його характеристики крізь призму світобачення юриста.

Існує безліч тлумачень Блокчейн технології, і всі вони відображають різні її аспекти. Оскільки Блокчейн є похідною технологією від Технології розподілених реєстрів, на кшталт бухгалтерських книг (“Distributed Ledger Technology” або “DLT”), найбільш поширеною є дефініція Блокчейну як *розподіленої бази даних*, у якій кожна транзакція та її деталі записуються одночасно у всіх користувачів (тобто на всіх вузлах) без центральної бази даних чи адміністратора (Peer-to-peer transmission) [1, с. 2]. При цьому записи здійснюються в одиниці обліку, в якій зашифровується розмір фізичного показника ресурсу, що, власне, і є предметом транзакції: одиниця вартості майна чи послуги, права допуску до системи, доступу до інформації чи іншого права чи зобов’язання (токен).

Поряд із цим Блокчейн також визначають як технологію, що забезпечує *управління невизначеною кількістю транзакцій, здійснених користувачами мережі безпосередньо* на основі консенсусу, і збереження цих транзакцій в криптографічно захищених одиницях інформації – *«Блоках»* [2, с. 3], *кожен з яких об’єднаний хеш значенням*, розрахованим за допомогою спеціального алгоритму на підставі даних про попередні блоки (майнінг). Вказаний процес складає так званий протокол проведення транзакцій в Блокчейн, який перевіряють користувачі та за умови правильності його дотримання консенсусом схвалюють його приєднання, після чого дані про транзакцію оновлюються у всіх блоках. Історія транзакцій доступна кожному, хто має програмний доступ до реєстру. Конкретна особа не має технічної можливості внести зміни до вже валідованого блоку інформації, оскільки будь-які зміни мають бути консенсусно узгоджені між учасниками шляхом однорангової передачі даних (для цього необхідна згода 51% учасників мережі). Для взаємодії в системі кожен користувач має пару ключів: приватний та публічний. Приватний ключ відповідає поняттю електронного цифрового підпису, тобто є унікальним для кожного користувача, та не доступний іншим, а публічний ключ використовується для шифрування повідомлень (транзакцій) та доступний всім учасникам мережі [3, с. 465].

Кожне із зазначених визначень відображає такі специфічні характеристики Блокчейн-технології, як децентралізація, незмінність записів, транспарентність, які, однак, мають ґрунтуватися на розумінні того, що це перш за все технологія організації даних за конкретним протоколом консенсусного прийняття рішення про проведення транзакцій. Саме консенсусний характер здійснення транзакцій у Блокчейн і є основною особливістю системи, що є підтвердженням її децентралізованої природи і таким чином гарантує транспарентність процесів, які в ній відбуваються, для всіх користувачів.

Залежно від протоколу та набору алгоритмів консенсусу, а отже, і розподілу прав учасників мережі, транспарентності доступу до інформації та швидкості проведення транзакцій зустрічаються різні моделі Блокчейн-технологій, зокрема публічний, приватний чи консорціумний [4, с. 3]; публічний без дозволу, публічний з дозволом, приватний без дозволу та приватний з дозволом [5, с. 163]; відкрита участь\відкритий запис,

відкрита участь\запис за дозволом, закрита участь\запис за дозволом [1, с. 4], публічні децентралізовані мережі, публічні мережі з децентралізованим управлінням, приватні мережі, що контролюються, державні мережі [6, с. 40]. Таке групування в основному здійснюється за 4 характеристиками:

публічність – доступ до мережі з правом зчитувати дані має будь-який користувач (вузол);

приватність – доступ до мережі з правом зчитувати дані мають лише користувачі звизначеною ідентичністю, члени однієї спільноти, компанії, в результаті чого забезпечується конфіденційність інформації в мережі, а сама мережа має вищий ступінь довіри;

Відповідну ідентифікацію може проводити так званий адміністратор (пул адміністраторів), тобто суб'єкт, який формує приватну мережу, або відповідні критерії ідентифікації можуть бути прописані в коді доступу до мережі (консорціумна модель).

відсутність дозволу – *валідувати*, тобто здійснювати перевірку транзакцій на відповідність правилам протоколу та підтверджувати їх, а також вносити дані до розподілених записів може *будь-який користувач*;

наявність дозволу – *валідувати*, тобто здійснювати перевірку транзакцій на відповідність правилам протоколу та підтверджувати їх, а також вносити дані до розподілених записів можуть *тільки визначені користувачі*.

Слід відзначити, що полярні набори відповідних ознак формують моделі Блокчейн з абсолютно різними можливостями та недоліками. Так, публічний Блокчейн, який не передбачає отримання дозволу на верифікацію, вважається найбільш транспарентним та надійним, адже відповідність протоколу кожної транзакції встановлюється невизначеним колом користувачів, кожен з яких має право записувати дані, а отже, вимагає багато часу та потужності системи, водночас приватний Блокчейн, який передбачає отримання дозволу на верифікацію, характеризується значно нижчою «демократичністю» (вхід до мережі, а також відповідність транзакції залежить від конкретних суб'єктів або програмних ідентифікаторів), але виграє за рахунок високої швидкості проведення транзакцій та гарантування конфіденційності даних у мережі.

Американський юрист з корпоративного права Джуліо Корраджіо вказує на такі переваги і недоліки двох різних видів мереж, одна з яких містить систему авторизації, а інша – ні: оскільки авторизована мережа фактично контролює рівень доступу користувача до системи, її законність та відповідність забезпечити значно легше. Проте вищий рівень контролю значною мірою впливає на транспарентність публічних мереж, яка вважається однією з основних переваг технології Блокчейн. У даному випадку немає правильного або хибного рішення. Воно має бути прийняте з огляду на цільове призначення того чи іншого ланцюга [7].

Існує думка, що в мережі із системою авторизації (приватній), в якій адміністратор ідентифікується, на адміністратора може бути накладено централізовану відповідальність за події, що відбуваються на платформі. Натомість у мережі без авторизації (публічній) йтиметься про розподіл відповідальності рівною мірою між усіма учасниками мережі. Нерозуміння технічних аспектів різниці між авторизацією доступу та валідуванням транзакції, а також накладення на це хибного розуміння правової інтерпретації веде до сумнівних висновків. Так, контрольований доступ у першому варіанті зовсім не означає, що адміністратор може контролювати всі події в ланцюгах, так само як безконтрольний доступ у другому варіанті не дає підстав накладення відповідальності на усіх користувачів ланцюга, які не мали відношення до конкретної транзакції, що може набувати ознак правочину.

Виділяють два підходи до встановлення відповідальності за помилки в програмному коді Блокчейн: абсолютну та обмежену відповідальність. Стосовно першої розробники відкритих кодів (публічних мереж) вказують, що з технічної точки зору є значні ризики втручання, а отже, їм стає невиправдано дорого включати фінансове забезпечення відповідальності в ціну продукту, що може призвести до згортання таких пропозицій. Разом із тим забезпечення обмеженої їхньої відповідальності може створити лазівку для суб'єктів, які пропонують інші програмні продукти, видаючи свої програми за Блокчейн з відкритим кодом. Як середнє рішення пропонується встановити обмежену відповідальність, настання якої могло б ґрунтуватися на недотриманні стандартів та кращих практик безпеки і якості написання кодів [8, с. 47-48]. Таким чином, правове забезпечення відповідних відносин має бути сформоване на чіткому розумінні всієї багатоманітності технологічних можливостей Блокчейну.

Блокчейн як технологія організації даних найчастіше функціонує не сама по собі. Вона поєднується з різноманітними програмними кодами, які визначають логіку проведення транзакцій мережі, гарантуючи їх повну автоматизацію. Програми, які становлять заздалегідь передбачені алгоритми, що починають діяти за умови дотримання узгоджених

правил, автоматично запускаючи транзакції між вузлами, мають назву смарт-контрактів. Слід відзначити, що у відповідних кодах втілені умови, настання яких учасники погодили як підставу автоматичного виконання транзакцій. Вказаний код з відповідними умовами міститься в блоках усіх учасників, що гарантує йому високий рівень надійності та незмінності, а також детермінованості виконання настанням вказаних умов, наприклад час проведення конкретної транзакції.

У цьому аспекті дозволимо собі зробити кілька юридичних коментарів. З одного боку, смарт-контакт за юридичним складом може розглядатись як правочин в актуальному визначенні законодавства України (дії особи, спрямованої на набуття, зміну або припинення цивільних прав і обов'язків) [9], а саме, в ньому присутні такі елементи:

– *сторони / підписанти* – контрагенти, які мають певні домовленості між собою. Для засвідчення волі сторін можливе використання електронного цифрового підпису або мультипідпису за наявносі великої кількості контрагентів;

– *предмет* – активи, які мають знаходитися всередині системи реалізації смарт-контракту або мати відповідний зв'язок з ним (наприклад, у смарт-контракті має бути передбачена система цифрового інформування банку, де перебувають активи, про виконання сторонами угод, які дозволяють банку здійснити відповідну транзакцію);

– *умови* – перелік алгоритмів, у разі виконання яких сторони вважатимуть контракт виконаним.

З іншого боку, як слушно вказує Silvia Petruchino, смарт-контракт може бути настільки розумним, наскільки люди пропишуть відповідний код. Мається на увазі, що в коді можна прописати лише такі умови, які не допускають дискреції та різниці в тлумаченні [5, с. 163]. З огляду на вказане, смарт-контракти розуміють як спосіб виконання традиційних юридичних договорів, наприклад як найпоширеніший з них – переказ коштів між контрагентами.

Незмінність коду та детермінованість є безцінними властивостями для виконання умов юридичного договору та відкриває величезні можливості для подолання хронічної хвороби невиконання юридичних договорів, але разом із тим містить у собі суттєвий недолік, який полягає в ригідності до зміни обставин виконання зобов'язань, зумовлених зміною відносин між учасниками юридичних договорів, наприклад, для виконання яких його було прописано. Вказані обставини відкривають широке поле юридичних питань.

З точки зору загальних вимог, додержання яких є необхідним для чинності правочину, технологічні властивості не можуть гарантувати їх дотримання. Так, вимога до форми правочину є не вирішеною, адже зрозумілі комп'ютеру команди (алгоритми), за допомогою яких виконується воля сторін, можуть розумітися як письмова, як усна або навіть як особлива форма. Можна припустити застосовність до смарт-контракту принципу свободи договору, включаючи свободу його форми, але все ж, на нашу думку, більш визначеною є позиція законодавця Італії, який у ч. 3 ст. 8 Закону від 11.02.2019 прямо вказав, що електронні документи набувають юридичного значення з моменту запису про їх зберігання в розподілену базу даних [8, с. 60]. Крім того, використання ключів для ідентифікації не завжди дає можливість встановити правовий статус контрагентів, а отже, застосувати належні правові норми, наприклад визначити, чи є правочин споживчим та чи необхідно застосовувати до нього відповідне законодавство, а також чи взагалі володіє контрагент необхідним обсягом правосуб'єктності (малолітня особа, недієздатні тощо). Не можна виключати в цьому контексті й кіберризики. Так, беручи до уваги той факт, що однорангові мережі є децентралізованими, існує два способи ідентифікації нового учасника мережі: отримати гарантії його сумлінності від інших учасників мережі або перевірити його самостійно. Однак у міру масштабування крипто-мережі вимога до кожного учасника підтверджувати власні ідентифікаційні дані стає недоцільною, що призводить до утворення так званих ідентифікаторів-псевдонімів, які використовуються для заплутування учасників мережі, що має назву атака Sibyl. Що більше ідентифікаторів належить зловмиснику, то більше шансів, що наступну транзакцію сумлінний учасник здійснить на користь зловмисника.

Не завжди також зрозуміло, як гарантувати виконання в реальності, наприклад, правочину про передачу права власності на частину супутника, якщо обидва контрагенти та інші учасники мережі, які валідують транзакцію, можуть не знати напевно, чи такий існує насправді. Для вирішення відповідних питань нині держави залучають нотаріусів (примітною в цьому контексті є Італія з приватною Блокчейн мережею Notarchain [10]) або так званих «фізичних валідаторів», які відповідають за те, щоб покупець токену дійсно придбав товар із легальною передачею основного юридичного права чи обов'язку [11].

Ще одним цікавим питанням у зв'язку з виконанням умов смарт-контрактів є вирішення спорів між сторонами, яке

в межах мережі виглядає доволі проблематично внаслідок рівності всіх учасників мережі, а отже, чужорідності самого поняття «суддя» чи «арбітр», який наділений владою визначати дії інших. У цьому контексті Silvia Petruchino пропонує використовувати арбітражні угоди, зокрема ту частину, яку об'єктивно не можна передати як код, відобразити в юридичній угоді, а іншу – передбачити власне як арбітражний смарт-контракт, зміст якого може полягати у введенні у мережу адміністратора, який перевірятиме код та додаватиме інформацію про транзакцію у разі, якщо визначить, що попередня була проведена не відповідно до протоколу або без урахування обставин об'єктивної дійсності [5, с. 174]. Вказана пропозиція може бути застосована лише у мережах з наявністю дозволу та орієнтована на так зване «судочинство», влада якого походить із добровільного погодження сторін, тобто договору. З цієї позиції доречно припустити, що відповідні умови можуть бути прописані й у третейській угоді, частина яких буде відображена у формі коду смарт-контракту.

Поряд із цим відповідна ідея все ж містить ризики централізації мережі Блокчейн та втрати нею іманентних ознак, які визначають її сутність. Якщо мережа децентралізована, то база даних має зберігатися в багатьох судових органах, зокрема, різних держав у разі вирішення міжнародних спорів. Крім того, необхідно переконатися, що держава, до якої належить інша сторона, також послуговується технологією розподілених даних у судочинстві. Якщо говорити про організацію державних судів на засадах Блокчейн, є сенс передбачити загальнодержавну розподілену базу даних судових рішень на кшталт тої, що створена для нотаріату, і є сенс говорити про відповідні зміни до процесуальних кодексів.

Ще однією особливістю смарт-контрактів є локалізованість їхньої дії, тобто тільки в межах мережі. Разом із тим для запуску коду чи виконання певних операцій необхідні дані, яких просто не існує в мережі. Так званий зв'язок із зовнішнім світом забезпечується за допомогою спеціальних сервісів, часто з використанням хмарних обчислень, які надсилають та перевіряють дані із зовнішніх електронних джерел за межами Блокчейн мережі, передаючи дані до смарт-контрактів, таким чином уможливлюючи їх виконання (оракли). Оракли здатні працювати з різними типами даних і форматують їх для подальшого використання у мережах Блокчейн. Нині серед відомих типів ораклів можна зазначити три основні: для збереження даних про певні події (зокрема, даних про температуру, тиск, вологість у певному приміщенні), для прогнозування (зокрема, коливання цін на фондових біржах), для фіксації приватних даних (зокрема, персональних даних або даних про право власності) [12, с. 53].

Вказаний сервіс допомагає певним чином вирішити вищевказану проблему ригідності умов смарт-контрактів стосовно змін поза Блокчейн мережею, але слід пам'ятати й те, що вказаний сервіс тільки зчитує дані, які були занесені в систему людиною. Навіть у випадку перевірки, здавалось би, таких не залежних від людини даних, як погода, що стає умовою виконання смарт-контракту, існує можливість внесення людиною помилкових змінних для обчислення даних про погоду в мережу, в якій оракл перевіряє цю умову для виконання смарт-контракту. Отже, так званого людського фактору уникнути все одно не вдасться, а тому він має керуватися іншим чином поза мережею Блокчейн.

Висновки

Проведене дослідження дає підстави зробити такі висновки:

1. Блокчейн є технологією організації даних за конкретним протоколом консенсусного прийняття рішення про проведення транзакцій, якій притаманні ознаки транспарентності та незмінності валідованих даних. Разом із тим, залежно від цілей користувачів, її можна організувати як публічну або приватну, з дозволом чи без дозволу на проведення транзакцій, що робить цю технологію цінною для контролю над операціями самими користувачами на необхідному для них рівні транспарентності.

2. За даними усталеної практики застосування смарт-контракту, ця технологія сприймається її користувачами як цифровий аналог договірних зобов'язань або цифрова гарантія реалізації реального договору. Завдяки смарт-контракту, реалізуються три основні юридично значимі функції Блокчейн: реєстрація угод, ідентифікація контрагентів і третіх осіб та укладення договорів між сторонами. З правової точки зору смарт-контракт може бути визнаний правочином, зокрема, завдяки наявності в його структурі таких істотних елементів, як сторони, предмет та умови правочину. З іншого боку, смарт-контракт може виконувати суто роль інструменту для виконання правочину в кожному з таких випадків: 1) криптографічна форма укладення договору не передбачена нормами законодавства держави, між суб'єктами якої укладається правочин, або низки держав, якщо правочин укладається між суб'єктами господарювання, зареєстрованими під юрисдикцією різних держав;

2) криптографічна форма укладення договору законодавчо не прирівнюється до письмової форми договору; 3) функціонування та застосування технології Блокчейн і смарт-контракту як її похідного інструменту в принципі не регламентується відповідними нормами законодавства. У такому разі, якщо в законодавстві держави / держав реєстрації сторін смарт-контракту не існує прямих заборон на укладення правочинів або певних їх видів у криптографічній формі, смарт-контракт може бути застосований лише як інструмент виконання правочину цілком або в певній його частині.

3. Для введення смарт-контракту в правове поле необхідно врегулювати як мінімум такі питання, як визначення криптографічної форми правочину, механізми ідентифікації суб'єкта та захисту їх від неправомірних дій в мережі, а також ідентифікації предмета цих правочинів, зокрема, за допомогою визначення відповідних уповноважених осіб (нотаріусів чи валідаторів).

4. Разом із тим варто пам'ятати, що впровадження смарт-контракту технічно неможливе без впровадження технології розподілених реєстрів (DLT), зокрема Блокчейн, оскільки початково смарт-контракт був розроблений як комп'ютерний алгоритм, за допомогою якого здійснюється контроль і надається інформація про володіння певними активами саме в мережі Блокчейн. Так само є беззмістовним впровадження технології Блокчейн без впровадження смарт-контракту, що позбавляє мережу повноцінного й одного з основних інструментів її функціонування. Крім того, не варто випускати з поля зору й інший інструмент – оракл, який компенсує суттєвий, але вимушений з точки зору безпеки недолік, пов'язаний із замкненістю мережі суто на даних, наявних в її межах, адже саме завдяки ораклу стає можливим отримання суттєвих для здійснення правочину даних із зовнішніх ресурсів.

5. Зазначені аргументи обґрунтовують необхідність законодавчого визначення усіх перерахованих технічних явищ (технології розподілених реєстрів, Блокчейн, смарт-контракт, оракл), а також доводять, що регламентація деяких із них із повним або частковим ігноруванням усіх інших має потенціал створити правові лакуни і мертві норми, замість полегшення і осучаснення правовідносин між суб'єктами-користувачами мережі, оскільки норми законодавства мають бути логічним і ефективним продовженням фактів об'єктивної дійсності.

6. У процесі законодавчого визначення і регламентації використання смарт-контракту варто приділити особливу увагу поняттям приватного і публічного ключів, а також визначенню відповідальності за неправомірне їх використання, оскільки саме за допомогою зазначених ключів відбувається так зване «асиметричне шифрування» даних про користувачів та їхнє волевиявлення, а використання приватного ключа за своєю природою має багато спільного зі звичним для законодавства і цифрової інфраструктури України методом електронного підпису.

7. Мережа Блокчейн здатна забезпечити верифікацію технічної достовірності й актуальності даних, але не правомочність закладених у смарт-контракті юридичних умов, що залежатиме суто від особи, яка викладала такі умови з правової точки зору, та іншої особи, яка трансформувала їх у криптографічний код. За таких обставин основна функція Блокчейн буде обмежуватися суто захистом від несанкціонованого доступу до даних і припиненням спроб незаконного внесення змін до існуючого реєстру даних. Іншими словами, в рамках реєстрів, сформованих на основі Блокчейн, та у смарт-контрактах існує не поняття законності дій, а лише відповідність певним алгоритмам самої системи, що повертає нас до питання людського фактору. Відповідна помилка може бути допущена як правниками, так і технічними фахівцями, що зрештою може спричинити неперерахування активів від одного суб'єкта іншому. Викладена проблема потребує поглибленого предметного вивчення і деталізованих сценаріїв врегулювання, які необхідно напрацьовувати із залученням досвідчених фахівців у галузі як юриспруденції, так і IT-технологій.

Список використаних джерел:

1. Karen J. Jones Blockchain in the Space Sector. *Center for Space Policy and Strategy*. March 2020. 17 p.

2. Mohamed Torky, Tarek Gaber, and Aboul Ella Hassanien Blockchain in Space Industry – Challenges and Solutions. 27 p. URL: www.egyptsceince.net (дата звернення: 15.07.2020).

3. Кравченко П. Блокчейн і децентралізовані системи : навчальний посібник : у 3 ч. Ч. 1 / П. Кравченко, Б. Скрябін, О. Дубініна. Харків : ПРОМАРТ, 2019. 452 с.

4. Rohit Mital, Jack de La Beaujardiere, Rohan Mital, Marge Cole, Charles Norton. Blockchain application within a multi-sensor satellite architecture. URL: https://ntrs.nasa.gov/search.jsp?R=20180006549. 15 p. (дата звернення: 20.07.2020).

5. Silvia Petruzzino Blockchain and Smart-Contracts: a New Challenges for International Commercial Arbitration. Czech Yearbook of Arbitration. Arbitration and International Treaties, Customs and Standarts, 2020, Volume X. P. 161-179.

6. Кудь О., Кучерявенко М., Смичок Є. Цифрові активи та їх правове регулювання у світлі розвитку технології блокчейн : монографія. Харків: Право, 2019. 216 с.

7. Giulio Coraggio. What is the liability deriving from the blockchain? And how to handle it? Gaming TechLaw. URL: https://www.gamingtechlaw.com/2016/05/liability-blockchain.html (дата звернення: 15.07.2020).

8. Study on Blockchains Legal, governance and interoperability aspects (SMART 2018/0038). 218 p. URL: https://ec.europa.eu/digital-single-market/en/news/study-blockchains-legal-governance-and-interoperability-aspects-smart-20180038 (дата звернення: 03.08.2020).

9. Цивільний кодекс України : Закон України від 16.01.2003 № 435-I-V / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 03.08.2020).

10. Applicazioni Diditali: Ecco la "Notarchain". URL: https://consiglionotarilemodena.it/applicazioni-digitali-ecco-la-notarchain/ (дата звернення: 03.08.2020).

11. Token- und VT-Dienstleister-Gesetz (TVTG) Dieses Gesetz tritt unter Vorbehalt der Erfüllungder verfassungsrechtlichen Voraussetzungen am 1. Januar 2020 in Kraft. URL: https://impuls-liechtenstein.li/wp-content/uploads/2019/11/950.6_TVTG_25.10.2019.pdf (дата звернення: 03.08.2020).

12. Карпиловский Д. Б. Биткойн, блокчейн и как заработать на криптовалютах. Москва : АСТ, 2018. 256 с.

Anna Hurova, Mariia Kirpachova. Legal aspects of the Blockchain application in space activity: the key elements and models of the technology organization

This is the opening article in the series of publications dedicated to in-depth study of legal nature of the DLT (distributed ledger technologies), and in particular its most popular example Blockchain. The article is intended to establish basis for the further substantive highlighting of the research results related to application of the distributed ledger technology in space activities and adequate reflection of these processes in the legislative framework of Ukraine. The article provides interpretation of the main elements of the above mentioned technology in terms of jurisprudence, as well as analyzes the potential difficulties that can arise in the process of Blockchain implementation into the legal background of various industries. Thus, both the types of the technology system itself (public or private, permissioned or permissionless, methods of the new network users` validation) and its derivatives (namely smart-contracts and oracles) are studied. The problem of the technology application as the mean to exercise the space actors` rights and responsibilities is also discovered in the framework of the current research. In particular, much attention is paid to the legal features due to which the smart-contract can be considered as a plea with further identification of its parties. The research also deals with ways to protect the rights of less aware and therefore vulnerable users of the Blockchain network, liability emerging in case of technical error in the software code or as the consequence of cyber attack. At the same time, the issue of the cryptographic form of the plea and its recognition at the legislative level is being studied in detail. Special attention is paid to the issue of dispute resolution between the parties of the smart-contract, feasibility of engaging a judge or arbitrator into the network, as well as reconciliation of such a role with the concept of peer-to-peer relations between the participants of the network. In addition, the research addresses the issues of the oracle tool applicability, aimed at obtaining fixed data from resources outside the network, in order to solve the problem of network constraints when performing transactions. In general, the research demonstrates interpenetration of the Blockchain technical aspects and the range of legal relations that are currently being implemented and have the potential to be performed on the basis of this platform in the legal framework of foreign countries and Ukraine.

Key words: Blockchain, distributed ledger technology, nod, peer-to-peer transactions, token, hash value (code), private key, public key, validation, oracle.